Nova Law Review

Volume 23, *Issue* 2 1999 *Article* 7

The Brave New World of Banking on the Internet: The Revolution of our Banking Practices

Jacqueline Marcucci*

*

The Brave New World of Banking on the Internet: The Revolution of our Banking Practices

TABLE OF CONTENTS

I. INTRODUCTION

The electronic medium of communication known as the Internet is rapidly becoming the home of a new virtual economy. Using the Internet, a consumer has the ability to purchase products and receive goods in the privacy of the home. This new ability to buy and sell goods online is quickly becoming a major component of electronic commerce. It is within electronic commerce that financial institutions have shifted to Internet-based electronic banking.[1] Internet-based electronic banks and Internet banking open the doors for financial institutions to attract new customers and lower the institutions' overall costs.[2]

1. Bret G. Wilson, *Banking on the Net: How to Get Your Financial Services Client There with Minimal Trouble*, 43 PRAC. LAW. INST. CORP. L. HANDBOOK SERIES 25, 26 (Mar. 1997).
2. *Id.*

Initially, financial institutions only had Internet or Web pages with general information about banks.[3] Banks expanded their Internet Web sites to provide consumers with the ability to conduct their banking transactions via the World Wide Web and the Internet as both banks and consumers increased their Internet usage.[4] Banking on the Internet has created several choices of electronic alternatives to conventional forms of money, and banking services by financial and nonfinancial institutions.[5] Electronic banking includes electronic fund transfers and electronic payment systems. It also includes banking services provided by financial institutions as well as nonfinancial institutions. The nonfinancial institutions are often referred to as nonbanks.[6] There are a number of nontraditional entrants in the banking industry, including AT&T and Microsoft, that are competing with traditional banks.[7] Currently, there are three different types of electronic banking.[8] The first is "online banking," where an individual connects to a traditional bank's private network to perform conventional banking transactions.[9] The second is "web-based banking," where an individual connects to a traditional bank over the public Internet to perform conventional banking transactions.[10] The third type of electronic banking is through an actual "Internet bank."[11] The Internet-based bank focuses on providing bank-like services without the conventional structure, or even building of a traditional bank.[12] Internet-based banks offering services solely on the Internet are also competing with the traditional banks. Because of such diversity in electronic banking, its role within electronic commerce has changed tremendously within a short amount of time. In particular, there is an increasing presence of electronic money on the Internet, which is slowly impacting the entire financial industry.

"Electronic cash . . . refers to any electronic notation for money."[13] Since electronic cash is the currency of the Internet, it promises to have a wide impact on bank supervision and monetary policy. Electronic money is

---

3. Kimbrelly Kegler, *Electronic Banking: Security, Privacy, and CRA Compliance*, 2 N.C. BANKING INST. 427 (1998).

4. *Id.*

5. Marty Fisher-Haydis & Kara R. Yancey, *Developments in Banking Law: 1996*, 16 ANN. REV. BANKING L. 76, 92 (1997).

6. *Id.* at 99.

7. Dan L. Nicewander, *Electronic Banking—Smart Cards, Cyberspace and the Internet*, 50 Consumer Fin. L. Q. Rep. 22 (1996).

8. Kegler, *supra* note 3, at 426.

9. *Id.*

10. *Id.*

11. *Id.*

12. *Id.*

13. Fisher-Haydis & Yancey, *supra* note 5, at 76.

being marketed as a mechanism to facilitate commerce. This market can be very lucrative, especially in light of the growth of the Internet. At the end of 1997 there were thirty million worldwide users of the Internet and thirty-five million households in the United States with personal computers.[14] In December 1998, NUA, an Internet statistics company, reported that there were 151 million worldwide Internet users, or three percent of the world population, with over seventy-three million Internet users in the United States.[15] It is speculated that electronic money will replace approximately 400 billion dollars of the United States' currency circulating worldwide.[16] Indeed, it is predicted that the amount of cash in circulation will continue to fall from 400 billion dollars to 200 billion dollars by the year 2005.[17] Without a national monetary policy that manages "electronic money," such money will potentially make the money supply infinite because electronic money could possibly be infinite. Our current monetary policies and regulatory agencies are not structured to deal with "electronic money," its liquidity, and origination.

Internet banking presents new legal and regulatory issues regarding banks and nonbank entities and their ability to gather, transfer, and store money. The federal and international agencies that regulate banks are faced with the problem of trying to apply existing regulations to banking on the Internet or create new regulations. The banking functions being performed on the Internet pose both legal and regulatory challenges.[18] Regulating the movement of money and transactions is much more complex than regulating a bank's web page. New regulatory issues also arise from using nonbank entities to store money on the Internet. Additionally, the two key issues of privacy of confidential information and security of financial transactions must be addressed.[19] This article will focus on banking on the Internet, and specifically the role of nonbank entities, privacy and security issues in electronic banking, and regulatory issues regarding banking on the Internet.

---

14. Catherine Lee Wilson, *Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond*, 30 CREIGHTON L. REV. 671, 673 (1997).

15. *NUA Internet Statistics* (visited Dec. 28, 1998) <http://www.nua.ie/surveys/how_many_online/index.html>.

16. D. Lee Falls, *Dateline 2005: Does Banking on the Internet Need to be Regulated?* 14 BANKING POL'Y REP. No. 24 1, 10 (1995).

17. *Id.*

18. Melanie L. Fein, *The New Business of Banking: What Banks Can Do Now*, 912 PRAC. LAW. INST. CORP. L. PRAC. COURSE HANDBOOK SERIES 91, 95–96 (1995).

19. *Id.* at 95.

II. INTERNET-BASED BANKS

One of the most significant features of the Internet is the ability to eliminate geographic barriers. It is this unique nature of the Internet that allows a financial institution, as well as a nonfinancial institution, to exist solely on the Internet. There are no brick walls, tellers, and no branch offices. Services are offered twenty-four hours a day. Such advantages of Internet-based banks are growing, but there are disadvantages for both the consumer and the financial institution. For instance, one disadvantage for the financial institution is that it is subject to uncoordinated and inconsistent regulations by states because the financial institution offers banking services over the Internet to customers in various states and across the world. Furthermore, the Internet-based bank must comply with the Community Reinvestment Act ("CRA")[20] because the CRA mandates that any Federal Deposit Insurance Corporation ("FDIC") insured bank must address and service the community needs in which the bank operates.[21] Being able to determine exactly what constitutes the "community" on the Internet is a challenge that all Internet-based banks face.[22]

While there are more than 840 banks that have Internet sites, the Office of Thrift Supervision has granted thrift charters to only two Internet-based banks, Security First Network Bank[23] and Atlanta Internet Bank.[24] The Office of the Comptroller of the Currency ("OCC") has also approved the charter for CompuBank, N.A.[25] The Security First Network Bank and the Atlanta Internet Bank offer all of their services over the Internet. It appears that such banking services will be able to compete with the larger banks, such as Citibank and NationsBank, because more customers may be reached and "fewer bricks mean higher returns."[26] With reduced costs, the Internet-based bank can offer better interest rates on money market accounts, certificate of deposits, and even checking accounts.[27] Indeed, the customer base of Internet banks have grown tremendously. For example, Atlanta Internet Bank began with about twenty customers in late 1996, and now has

---

20. Consumer Reinvestment Act of 1977, 12 U.S.C. § 2901 (1994).

21. 12 U.S.C. §§ 2901–07 (1994); 12 C.F.R. § 25.11(b)(1) (1998).

22. The Security First Bank Network, an Internet bank based in Atlanta, concentrates its CRA efforts in the Atlanta community. *See* Kegler, *supra* note 3, at 438.

23. *Security First Network Bank* (visited Dec. 1, 1998) <http://sfnb.com>.

24. *Atlanta Internet Bank Home Page* (visited Dec. 24, 1998) <http://www.atlantabank.com> [hereinafter *Atlanta*] (as of Feb. 20, 1999, this site no longer available).

25. *See* New York Times (Cyber Times), *Fewer Bricks Mean Higher Returns at New Internet Banks* (visited Feb. 25, 1998) <http://www.pcn.com> [hereinafter *Fewer Bricks*] (as of Jan. 30, 1999 this site had changed).

26. *Id.*

27. *Id.*

approximately 6,500 customers with deposits totaling near $95 million.[28] Within eighteen months, Atlanta Internet Bank has acquired assets of $175 million.[29] Now eighty percent of Atlanta Internet Bank's customers are outside of Georgia and from twenty-one countries around the world.[30] Security First Network Bank is also growing, and has about $45 million dollars in deposits.[31] Moreover, these Internet banks enjoy the same Federal Deposit Insurance Corporation ("FDIC") protection for their depositors as traditional banks' customers receive.

While these types of banks, as well as any nonbanks, can offer many conveniences and advantages, the consumer should be aware of problems that lurk on the Internet. The FDIC cautions the consumer about companies "pretending to be banks offering unusually high interest rates," because such institutions may not be FDIC insured.[32] The FDIC recommends that the consumer find out about a particular financial institution before giving out personal information and conducting transactions.[33] The FDIC also suggests that a consumer should be skeptical about any Internet site or any advertisement that makes an offer that is too good to be true.[34] The consumer should be cautious about banking with international financial institutions, because such institutions may not be complying with all of the federal and state regulatory requirements, which may result in the institution being here today and gone tomorrow.[35] The FDIC offers an Internet site where a consumer can either find out if a financial institution is FDIC insured or report any suspicious activity.[36] The future of these types of banks is uncertain, but the technology allowing all banking services to be available at the stroke of a finger and in the privacy of the home is here to stay.

---

28. *Id.*

29. *CNN-Cyberbanks: Anytime, Anywhere* (visited Apr. 18, 1998) <http://cnn.com/TECH/computing/9804/18/online.banking/index.html>.

30. *See generally Atlanta, supra* note 24.

31. *Id.*

32. *Internet Banking and Shopping: Cyber-Buyer Beware* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/consnews/fal97/netbank.html>.

33. *Id.*

34. *Id.*

35. One such situation arose in Idaho. There, European Union Bank, a bank chartered in Antigua, promoted itself to the residents of Idaho. The State Department of Finance issued a cease and desist order on the grounds that the bank was soliciting deposits on the Internet to Idaho residents without being chartered to operate a bank or any other form of financial institution in Idaho. *State Business of Banking Laws and the Internet, 21st Century Banking Alert No. 97-9-10* (visited Jan. 29, 1998) <http://www.ffhsj.com/bancmail/ 21starch/ 970910.html>.

36. *Suspicious Internet Banking* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/suspicious/sspcious.html>.

III. INTERNET BANKING AND ITS MONEY SUPPLY

Electronic banking is not significantly different from traditional banking concepts and activities. It simply represents an alternative delivery system for traditional banking products.[37] Electronic banking is very broad in scope and includes electronic funds transfers, electronic payment systems, global financial and banking systems, and personal computer ("PC") access to bank services.[38] Until recently, traditional banks and banking services primarily used private networks to manage transactions for consumers, corporations, financial institutions, and other entities.[39] The Internet offers an additional, but public, network for these services and systems. Recently, there has been a shift to Internet-based electronic banking. Internet banking is currently a small part of the world of electronic banking. However, since Internet banking deals directly with the consumer market, it offers the greatest potential for growth. The transition to Internet-based banking has opened the door to many new technologies, financial opportunities, and forms of commerce. For instance, electronic money is the result of such new technology that has emerged as a potential new currency to be used by banks, consumers, and merchants on the Internet.[40] Some believe that this is the beginning of the end of money as we currently know it. James Gleich states:

> Cash is quaint, technologically speaking—unless you're impressed by intaglio-steel-plate-printed paper with embedded polyester strips (meant to inconvenience counterfeiters). Cash is expensive—tens of billions of dollars drain from the economy each year merely to pay for the printing, trucking, safekeeping, vending, collecting, counting, armored-guarding and general care and feeding of our currency. Cash is obsolete.[41]

But not everyone shares that view. The U.S. Department of the Treasury states:

---

37. *An Introduction to Electronic Money Issues*, prepared for the United States Department of the Treasury Conference, Toward Electronic Money and Banking: The Role of Government, September 19–20, 1996, Washington, D.C. [hereinafter *Electronic Money Issues*] (on file with author).

38. *Id.*

39. *Id.*

40. *Id.*

41. James Gleick, *The End of Cash* (visited Jan. 14, 1999) <http://www.around.com/money.html>.

> Conversion of Treasury payments, now running at about 800 million a year, to an all electronic format will bring changes permitting, for example, a consolidation of disbursing operations that currently produce checks. [A]mong the less technologically advanced countries, cash is the principal means of payment, the dollar seems to be one of the currencies of choice, and the infrastructure that will support widespread use of electronic money seems many years away.[42]

A. *What is Electronic Money?*

The term electronic money refers to the recording or storing of information about the funds or "value" available to a consumer.[43] This information is stored on a device in the possession of the consumer, such as a personal computer, or "smart card."[44] The device is then updated with information over either a private network or a public network, like the Internet.[45] For example, a phone card with a preset value of five dollars is a "smart card." While "smart card" technology is a type of electronic money, electronic money also includes "electronic cash." The advantages of electronic money are that it can: 1) offer new revenue streams for banks and other issuers or nonbanks in the form of fees; 2) "float" interest on balances stored and held by the issuer; and 3) cost savings from reduced cash handling costs.[46] Often, the term "electronic cash" is used interchangeably with the term "electronic money." Electronic money provides a means for consumers to purchase goods and for retailers to sell goods efficiently when using a credit card is not feasible or desirable.[47]

Several private companies have created "electronic money software products." Three such software products that facilitate the creation and management of electronic money are NetCash, ecash, and CyberCoin. These emerging products focus on balancing the privacy aspect of credit cards with

---

42. *Electronic Money Issues*, *supra* note 37.

43. *Id.*

44. *Id.*

45. *Id.*

46. *Implications for Central Banks of the Development of Electronic Money* (visited Jan. 14, 1999) <http://www.bis.org/publ/bisp01.htm>.

47. *Id.*

the anonymity of cash.[48] Currently, there is no one system that is universally accepted to make, issue, or manage electronic money.[49]

NetCash is a form of electronic money that is distributed by an online private bank, NetBank.[50] The customer sends United States ("U.S.") dollars to NetBank in exchange for a NetCash coupon.[51] The customer receives the coupon as an encrypted e-mail. It has three parts: "the 'NetCash U.S. $' keyword, the dollar amount, and the serial number of the bill."[52] When the customer wants to purchase a product, the customer sends a coupon to NetBank. Then, NetBank sends "digital coins" to the merchant as payment for the product.[53] The merchant also has an account with NetBank, and may then convert the "digital coins" back to dollars.[54]

DigiCash, founded in 1990, is a leading pioneer in electronic payment systems using public key cryptography.[55] DigiCash uses "ecash," a trademarked product specifically developed for the Internet, as a form of electronic cash.[56] Customers and merchants use the bank's public key to decode messages and conduct transactions.[57]

DigiCash uses ecash "coins" which have a specified value.[58] An electronic "purse"[59] is established for the customers and merchants. The coins are then moved between customer, bank, and merchant to complete transactions.[60] To receive the value, the payee confirms the validity of the coins by depositing them online into an ecash account. This transaction will not reveal the name or address of the payer because each ecash coin is secured by a high-level encryption method. Like bank notes, ecash can be

---

48. *North American Media Engines-Resource Centre-Articles-Net Money* (visited Mar. 15, 1998) <http://www.name.net/netmoneys.html> [hereinafter *North American Media*].

49. *Id.*

50. *Id.*

51. *Id.*

52. *Id.*

53. *North American Media*, *supra* note 48.

54. *Id.*

55. *Id.*

56. *DigiCash-Profile* (visited Jan. 14, 1999) <http://www.digicash.com/digicash/digicash/profile/index.html>.

57. *Id.*

58. *ecash - An Introduction to ecash* (visited Apr. 9, 1998) <http://www.digicash.com/ecash/intro/index.html>.

59. *Glossary of ecash* (visited Feb. 16, 1999) <http://www.digicash.com/ecash/docs/purse_manual/gloss.html>.

60. *DigiCash – How ecash Works Inside* (visited Apr. 8, 1998) <http://www.digicash.com/ecash/docs/works/> [hereinafter *How ecash Works Inside*].

withdrawn from and deposited into deposit accounts.[61] The "coins" include strings of digits, with each string corresponding to a different digital "coin."[62] Each coin has a denomination, or value, so that a purse of digital coins is managed automatically by the customer's ecash software.[63] The customer's ecash software chooses coins with the desired value from the purse on the PC and then sends them over the network. When the merchant's software receives the "coins," the software automatically sends the "coins" to the bank. To ensure that each coin is used only once, the bank records the serial number of each coin in its database. If no such serial number has been previously recorded, the bank stores it and informs the merchant that the coin is valid and that the deposit is accepted.[64]

DigiCash's use of ecash has now gone one step further in providing privacy and anonymity. DigiCash uses "blind signatures," which prevent the bank from recognizing a particular account.[65] Instead of the bank creating a blank coin, the customer's computer creates the coin at random.[66] The coin is put in a "digital envelope" and sent to the bank.[67] The bank then withdraws one dollar from the customer's account and creates one dollar in digital form, similar to an embossed stamp on an envelope, before returning it to the customer's computer.[68] The "blind signature" mechanism allows the validating signature to be applied through the envelope.[69] When the customer's computer removes the envelope, it has obtained a coin of its own choice, validated by the bank's stamp.[70] However, because the bank is unable to recognize the coin, "the bank cannot tell who made the payment."[71] Therefore, the customer is anonymous and privacy is maintained.

Another company that has developed electronic money is CyberCash, Inc. ("CyberCash"). CyberCash has developed a "CyberCoin" that can be

---

61. *Id.*
62. *Id.*
63. *Id.*
64. *Id.*
65. The bank creates unique blank digital coins and validates them with its special digital stamp. *How ecash Works Inside*, *supra* note 60. This would normally allow the bank to recognize the particular coins when accepted in a payment and thus tells the bank exactly which particular customer made a payment. *Id.*
66. *Id.*
67. *Id.*
68. *Id.*
69. *How ecash Works Inside*, *supra* note 60.
70. *Id.*
71. *Id.*

used for purchases ranging from twenty-five cents to ten dollars.[72] The "CyberCoin" provides a means of paying for smaller items, when using a credit card would be inefficient.[73] In other words, "CyberCoin" is the equivalent of pocket change.[74] CyberCash seems to be placing some much needed emphasis on making the electronic cash transaction cost effective.

A principal disadvantage of electronic money in most of the current products is that the mechanisms used to store values and perform transactions use an electronic medium; therefore keeping track of all the past transactions, certificates, and coins and preventing double spending, would require massive databases.[75] Furthermore, software technology would have to be used to prevent an electronic purse and all of its contents from being used over and over again.

Such money can also result in many issues for banks. As previously noted, the makers of this money may not be banks, but rather private companies that are acting as banks in some manner. Federal regulators of banks are faced with the challenge of possibly regulating such companies as traditional banks. Secondly, through encryption methods, the banks are receiving money and depositing "money," without being able to trace such money. This leads to the issue of whether such strings of characters are indeed "money," as society knows it to be.

B. *Is it Money?*

One question facing regulators is whether a string of characters constitutes "money." Traditionally, the federal government has had the power "to coin Money, [and] regulate the Value thereof."[76] "[T]he Federal Government has not [always] been the sole issuer of currency."[77] Private and state banks also issued money until 1913, when the Federal Reserve System was established as the central banking system.[78]

---

72. *CyberCash - Free Wallet* (visited May 16, 1998) <http://www.cybercash.com/cybercash/consumers/wallet.html>.

73. *CyberCoin: Micropayments Revolutionize Web Commerce* (visited Jan. 14, 1999) <http://www.cybercash.com/cybercash/services/cybercoin.html>.

74. *Id.*

75. B. Clifford Neuman & Gennady Medvinsky, *NetCheque, NetCash, and the Characteristics of Internet Payment Services* (visited Jan. 14, 1999) <http://www.press.umich.edu/jep/works/NeumNetPay.html>.

76. U.S. CONST. art. I, § 8, cl. 5.

77. Wilson, *supra* note 14, at 691.

78. *Id.*

Now, a new tender is being developed which involves private companies generating "money."[79] "Whether on a card or the hard drive of a personal computer, the current forms of electronic money involve the storage of 'value' which is exchanged for goods or services."[80] Examination of the underlying features and properties of electronic money is essential to determining whether electronic money is money or something else that needs to be defined and possibly regulated, or even eliminated.[81] It can be argued that "electronic money," as a stored value, is a form of private money that would be accepted as legal tender. "However, the new electronic money systems lack [some] essential" traits of money.[82] First, when executing a transaction using an "electronic value," instead of cash or private money, the transaction is not completed in a single step.[83] Unlike cash or private money transactions, "electronic value" transactions require merchants to submit the value to the issuing bank before they receive cash, with the electronic money moving through various complex systems before the transaction is completed.[84] Second, electronic money does not qualify as a substitute for private money, "because all current electronic money developments allow the holder of the stored value to redeem it for the national currency," whereas private money may not be redeemed as such.[85]

The question of whether electronic money is money also raises the issue of customer confidence regarding the circulation of "electronic money." Currently, a customer has confidence that a credit given by a bank is redeemable for cash. Such confidence is largely due to the regulatory scheme of the FDIC that protects against bank failure. There is a risk, that if a nonbank becomes insolvent consumers would not be protected, and thus would be susceptible to a complete loss of funds stored in the nonbank.[86]

Electronic money is invisible and lacks any physical characteristics. If electronic money is to gain the confidence of the customer, it must fall under regulatory schemes. Nonbank entities will issue "electronic value" in exchange for U.S. currency. Under our current scheme, the entity would have to qualify as a "bank" before federal banking regulators could examine and control the activities of the issuer. Assuming the entities issuing smart cards and other electronic forms of "electronic value" are not banks and are not currently covered by our federal banking regulations, the issue then

---

79. *Id.*
80. *Id.* at 690.
81. *Id.* at 691.
82. Wilson, *supra* note 14, at 692.
83. *Id.*
84. *Id.*
85. *Id.*
86. UNITED STATES DEP'T OF TREASURY, TOWARD ELECTRONIC MONEY AND BANKING: THE ROLE OF GOVERNMENT (1996).

becomes whether the bank regulatory agencies should govern such entities or if some other governmental agency should regulate them.

IV. THE ROLE OF REGULATORY AGENCIES

In the midst of advancements in using the Internet for banking services, federal and international banking regulators continue to evaluate their roles in managing and monitoring electronic commerce, money, and more specifically, electronic banking. As new technology emerges everyday, more and more regulatory agencies try to find ways to guide the institutions they govern. There are also interagency bodies, such as the Federal Financial Institutions Examination Council ("FFIEC") that are empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions.[87] The FFIEC plays an important role in disseminating wide-spread guidance among the federal agencies. There are also international groups, such as the Bank for International Settlement, ("BIS"), who try to promote standards and principles regarding banking. In the United States, the Federal Reserve System, the Office of the Comptroller of the Currency ("OCC"), and the FDIC have continued to address the development of electronic banking and money systems and the appropriate U.S. government involvement. These three agencies have different roles, but they all regulate financial institutions. The FDIC is an independent agency that focuses on insuring banks. The OCC focuses on chartering national banks, and is part of the Department of the Treasury. The Federal Reserve System is an independent agency that focuses on monetary stability. Although these agencies have separate and distinct purposes, they often work together to promote a secure national banking system. For example, the FDIC has regulations to ensure a bank is safe and sound in order to be insured, while the OCC has regulations to ensure our national banking system is secure and stable.

On the global front the Group of Ten Nations ("G-10") and the BIS, are taking an active role in the regulation, and management of electronic

87. "The Federal Financial Institutions Examination Council (Council) was established on March 10, 1979, pursuant to the title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630." The FFIEC is empowered to prescribe uniform principles, standards and report forms for the Board of Governors of the Federal Reserve System, ("FRB"), the Federal Insurance Corporation, ("FDIC"), the National Credit Union Administration ("NCUA"), the Office of the Comptroller of the Currency ("OCC"), and the Office of Thrift Supervision ("OTS"). *See FFIEC Mission Statement* (visited Dec. 21, 1998) <http://www. ffiec.gov/mission.html>.

banking.[88] Working together, these organizations must lead individuals, corporations, and banking entities through these changing times.

A. *The Bank for International Settlements and the Basle Committee*

The Internet is helping to drive the integration of financial markets worldwide. This integration depends highly on the world's banks, its regulators, and the system's overall financial stability. The world's oldest international financial organization that addresses globalization of financial markets is the BIS.[89] It primarily promotes the cooperation of central banks and fosters international financial stability.[90] The BIS is owned and controlled by central banks and other international financial institutions.[91] The Board of Directors is comprised of the Governors of the central banks of Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the Chairman of the Board of Governors of the United States Federal Reserve System.[92] As of March 1998, forty-five central banks have voting rights at the general meetings of the BIS.[93]

In promoting the stability of the international monetary and financial systems, the BIS has been involved in the efforts of such groups as the G-

---

88. *See generally Group of Ten, Electronic Money* (Visited Dec. 26, 1998) <http://www.bis.org/publ/gten01.html>.

89. *The Bank for International Settlements* (visited Dec. 26, 1998) <http://www.bis.org/about/prof-gh.htm> [hereinafter *Bank for International Settlements*].

90. *Id.*

91. *Id.*

92. *Id.*

93. Forty-five central banks included:

> all the G-10 central banks, namely those of Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom and the United States of America - and the central banks of Australia, Austria, Brazil, Bulgaria, China, the Czech Republic, Denmark, Estonia, Finland, Greece, Hong Kong, Hungary, Iceland, India, Ireland, Korea, Latvia, Lithuania, Mexico, Norway, Poland, Portugal, Romania, Russia, Saudi Arabia, Singapore, Slovakia, South Africa, Spain and Turkey, together with the Central Bank of Bosnia and Herzegovina, the Croatian National Bank, the National Bank of the Republic of Macedonia, and the Bank of Slovenia, which have been issued shares of the Bank pending a comprehensive settlement of all outstanding questions in connection with the legal status of the suspended Yugoslav issue of the Bank's capital.

Id.

10.[94] The G-10 is comprised of eleven industrial countries: Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Sweden, Switzerland, the United Kingdom, and the United States.[95] These countries consult and cooperate on economic, monetary, and financial matters.[96] In 1975, the G-10 set up a committee to improve collaboration between bank supervisors known as the Basle Committee on Banking Supervision ("Basle Committee").[97] The Basle Committee provides a forum of discussion on the handling of specific banking supervision issues, coordinates the sharing of supervisory responsibilities, and seeks to enhance standards of supervision.[98] The BIS has participated in G-10 meetings since the Basle Committee was formed, because the Governors of the G-10 central banks meet regularly at the same time as the Basle monthly meetings.[99]

In March 1998, the Basle Committee took an initial step in reviewing supervisory issues related to technological advances. The Basle Committee distributed an assessment of the risks, and recommended approaches to risk management in electronic banking and electronic money activities to supervisors worldwide.[100] The risk management document suggests that "operational risk, reputational risk, and legal risk [are] the most important risk categories for electronic banking and electronic money."[101]

The risk management document identified operational risk as a risk category that must be addressed in dealing with electronic banking and electronic money. "Operational risk arises from the potential for loss due to significant deficiencies in system reliability or integrity."[102] Operational risk

---

94. The General Arrangements to Borrow ("GAB") of 1962, under which 10 member countries of the International Monetary Fund ("IMF"), including Switzerland, agreed to make resources available to the IMF outside their quotas, led to the countries participating in the GAB being known as the Group of Ten ("G-10"). *Bank for International Settlements, supra* note 89. Since 1963, the G-10 has been a principal forum for discussion of international monetary questions. *Id.*

95. *Id.*

96. *Id.*

97. *See* Report from Basle Comm. on Banking Supervision, *The Year 2000: A Challenge for Financial Institutions and Bank Supervisors* (Sept. 1997) <http://www.bis.org/publ/bcb531.pdf> (as of Feb. 20, 1999 this site no longer available).

98. *Id.*

99. *Id.*

100. Basle Committee on Banking Supervision, *Risk Management for Electronic Banking and Electronic Money Activities* (visited Dec. 24, 1998) <http://www.bis.org/publ/bcbs35.htm> [hereinafter *Risk Management for Electronic Banking*].

101. *Id.*

102. *Id.*

includes security risks that have the potential of both external and internal attacks and misuse of a bank's computing system.[103] Controlling access to a bank's system has become increasingly difficult with the expansion of computer capabilities and the accessibility of a public network, such as the Internet. Not only is there a potential for tremendous monetary loss, but there is also the potential for tremendous liability in fraudulently created activities. Operational risk also includes risks associated with a bank's system design, implementation, and maintenance.[104] The rapid change in information technology poses the risk that a system adequate today will not be adequate tomorrow.[105] Even computer software given to customers for online banking can quickly become obsolete and require updates.[106] Further, involvement of customers increases the potential of customer misuse of products and services.[107] The amount of services and products that are available to the customer is expanding everyday. Customers must be educated about necessary security precautions that should be taken, or else the risk of a security breach is heightened. Operational risk also includes customer misuse of banking products and services.[108] An uneducated customer can unintentionally open the door for security breaches by conducting financial transactions in a non-secure electronic environment. Criminals may then gain access to the financial transaction. Such access may lead to financial losses both to the customer and to the bank.[109]

Another risk category is reputational risk, that is, "the risk of significant negative public opinion that results in . . . critical loss of funding [for the bank] or [a loss of] customers."[110] Reputational risk can arise from systems or products not working properly, or from a significant security breach.[111] It also can arise from mistakes, malfeasance, and fraud by third parties. Reputational risk can be significant for a single bank and can also be significant for the banking system as a whole. Such risk can lead to extreme public distrust of *any* bank's ability to conduct business on the Internet. This

103. *Id.*
104. *Id.*
105. *Risk Management for Electronic Banking*, *supra* note 100.
106. *Id.*
107. *Id.*
108. *Id.*
109. *Id.*
110. *Risk Management for Electronic Banking*, *supra* note 100.
111. *Id.*

distrust will hinder both the growth of banking on the Internet, and the growth of electronic commerce collectively.[112]

A third category of risk identified by the Basle Committee is the legal risk arising from violations of laws, rules, regulations, or prescribed practices.[113] Legal risk also involves the lack of established legal rights and obligations of parties in an electronic transaction.[114] Given the fact that electronic transactions and electronic money are relatively new, no one is sure of the rights and obligations of the parties involved, and what type of consumer protection applies to the transaction.[115] There is also a question regarding the validity of agreements reached through an electronic medium, because technological advances such as digital signature and encryption methods that validate an agreement are still evolving. Further, there is the risk of customer disclosure and inadequate privacy protection. Moreover, the Basle Committee points out that the traditional banking risks may also arise in banking on the Internet, especially with the use of electronic money.[116] Cross-border risks and issues can arise for banks as well.[117] Customers across national borders expose the banks to different and/or additional regulatory requirements.[118]

In assessing the risks above, the Basle Committee sets out possible steps that bank management can take to manage and control risks associated with banking on the Internet and the use of electronic money.[119] The Basle Committee suggests such measures as developing a security policy that lays out the bank's plan and defines the bank's security risk tolerance.[120] Putting various security measures into place, such as encryption, passwords, firewalls, virus controls, and employee screening can help to prevent both internal and external attacks, as well as the misuse of electronic money and financial transactions.[121] In deterring security issues, a bank should consider

---

112. *Id.*

113. *Id.*

114. *Id.*

115. *Risk Management for Electronic Banking*, *supra* note 100.

116. Traditional banking risks include credit risk, liquidity risk, interest rate risk, and market risk. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

120. *Risk Management for Electronic Banking*, *supra* note 100.

121. A detailed discussion regarding security measures can be found in Bank for International Settlements, *Security of Electronic Money*, Aug. 1996 <http://www.bis.org/publ/cpss18.html> [hereinafter *Security of Electronic Money*].

a combination of security measures as opposed to just one.[122] For example, a firewall[123] can screen, or even prevent incoming messages but it does not fully protect against virus-infecting programs that can be downloaded from the Internet.[124] A better solution would be to implement virus protection protocols and software that also integrates well with the firewall software. The Basle Committee suggested that in dealing with operational, reputational, and legal risks, a bank's management should communicate with staff members about key provisions regarding banking on the Internet, while the technical staff communicates with the bank management on how systems work and are designed.[125] Protocols for the evaluating and testing of products and services should be established and performed regularly, and should include educating customers on those products and services. While electronic banking and electronic money rely on external entities for hardware and software, banks should insist that such providers conduct regular testing and have fallback procedures in case of failure or invasion by criminals.[126] Basically, banks should constantly monitor and test their systems and keep abreast of the latest electronic banking technologies. The BIS and the Basle committee are both providing strong guidelines for nations to follow while at the same time promoting electronic banking.

B. *The Federal Reserve System*

"The Federal Reserve System is the central bank of the United States. It was founded by Congress in 1913 to provide the nation with a safer, more flexible, and more stable monetary and financial system; over the years, its role in banking and the economy has expanded."[127] The Federal Reserve Board, which governs the Federal Reserve System, has been willing to allow financial institutions to move forward with new technology, such as smart cards and electronic banking.

The Federal Reserve Board has taken other steps that will have an effect on the development of electronic banking and electronic money activities in the United States. For example, the Board approved a request by various holding companies and banks, subject to the Bank Holding

---

122. *Id.*

123. A "firewall" is a combination of hardware and software that screens and limits external access to internal systems connected to open networks such as the Internet. *Id.* at 12.

124. *Id.*

125. *Id.* at 13.

126. *Security of Electronic Money*, *supra* note 121 at 15.

127. *About Federal Reserve System* (visited Mar. 25, 1998) <http://www.bog.frb.fed.us/aboutfrs.html>.

Company Act,[128] to obtain a voting interest in Integrion Financial Network, LLC of White Plains, New York ("Integrion").[129] Royal Bank of Canada, Northwest Corporation, and Stichting Prioriteit ABN AMRO Holding and its subsidiaries requested to acquire more than five percent of the voting interest in Integrion.[130] The joint venture also includes twelve national banks,[131] one savings and loan holding company,[132] and Gemini Management Corporation, a subsidiary of International Business Machines Corporation ("IBM"). Integrion was organized to design, develop, and operate a data processing and transmission system, through which customers of banks can engage in home banking and other electronic financial services with the financial institution.[133] The Federal Reserve Board's order focused on the public benefits of allowing such a joint venture.[134] Since the proposed activities were data processing and transmission activities which were permissible for

128. The Bank Holding Company Act authorizes bank holding companies to engage in nonbanking activities provided that such activities are "closely related to [the business of] banking." The act also states that the bank's activities must "produce benefits to the public, such as greater convenience, increased competition, or gains in efficiency, that outweigh possible adverse effects, such as undue concentration of resources, decreased or unfair competition, conflict of interests, or unsound banking practices." Bank Holding Act, 12 U.S.C. § 1843(4)(c)(8) (Supp. 1998).

129. *Federal Reserve Press Release - December 2, 1996* (visited Jan. 14, 1999) <http://www.bog.frb.fed.us/boarddocs/press/BHC/1996/199612022/> [hereinafter *Press Release*].

130. *Id.*

131. The national banks included:

> Bank of America NT & SA; NationsBank, N.A.; Keybank, N.A.; Bank One, Columbus, N.A.; Mellon Bank, N.A.; Barnett bank, N.A.; First Bank, N.A.; PNC Bank, N.A.; Michigan National Bank; The First National Bank of Chicago; Comerica Bank – Ann Arbor, N.A.; and Fleet National Bank. Each of these national banks has applied to the Office of the Comptroller of the Currency of the Currency to invest in Integrion through an operating subsidiary of the bank.

Id.

132. The savings and loan holding company is Washington Mutual, Inc., that had to provide notice of its intent to be involved with Integrion with the Office of Thrift Supervision. *Id.*

133. Customers can connect to Integrion, which serves as a gateway to the financial institution, using such devices as personal computers, touch-tone phones, or any other electronic communication devices. *Id.* The customer can connect through a private communication network, through financial software programs, or through the Internet. *Press Release*, *supra* note 129.

134. *Id.*

bank holding companies,[135] the Federal Reserve Board believed that such a venture would enhance consumer banking convenience by expanding the availability of remote banking services and providing new services.[136] Such a venture is also advantageous for financial institutions, because Integrion offers a secure means of banking online,[137] as well as a selection of software or programs for home banking.[138] As stated by the chairman and CEO of IBM, Integrion will reach sixty million households and give those sixty million people a reason to use the Internet for home banking.[139] Through policy, the Federal Reserve is encouraging the use of electronic banking at this time, while it monitors the effect on the United States economy and its financial systems.

C. *The Federal Deposit Insurance Corporation*

The FDIC has been insuring deposits and promoting safe and sound banking practices since 1934.[140] The FDIC:

---

135. Engaging in data processing and data transmission activities is permissible under section 225.28 of the Federal Reserve Board's Regulation Y, 12 C.F.R. § 225.28 (1998) and section 4(c)(8) of the Bank Holding Act. 12 U.S.C. § 1843 (c)(8) (Supp. 1998).

136. *Press Release*, *supra* note 129.

137. Integrion solves many security issues by providing both public Internet access as well as private networks. *15 North American Banks and IBM Form Company to Offer Electronic Banking and Commerce Services* (visited Sept. 9, 1996) <http://www.ibm.com/News/bankingpr.html>.

138. The customer can choose from whatever financial management software or Internet browser program he or she would like to use. Integrion is intended to be compatible with such software as Microsoft Money, Quicken and Managing Your Money, as well as Internet browsers like Netscape Navigator and Microsoft Explorer. *Id.*

139. Amanda Meffert, *Banking by IBM* (visited Jan. 4, 1999) <http://www.worth.com/articles/Integrion.html>.

140. *FDIC Symbol of Confidence* (visited Feb 17, 1999) <http://www.fdic.gov/consumers/symbol/index.html> [hereinafter *Symbol of Confidence*]. The FDIC was created to "restore stability to a financial system that had seen over 9,000 bank failures and a severe contraction in economic activity in the four years following the stock market crash of 1929." *Id.* "But in passing this legislation, President Roosevelt and Congress became concerned about the potential for deposit insurance to create 'moral hazard,' which is the tendency of people to take on more risk when insured" and reduce their incentive to monitor and discipline banks for excessive risk-taking. *Id.* Consequently, to limit the potential loss to the government, "the legislation limited the amount of insurance—to $2,500 in 1934, $5,000 in 1935—and increased the amount of federal supervisory authority over insured institutions (FDIC 1984)." *Confidence for the Future: An FDIC Symposium* (visited Dec. 26, 1998) <http://www.fdic.gov/publish/symp/backpap/panel1.html> [hereinafter *Confidence for the Future*]. "For the next 50 years, public confidence in the banking system was maintained even through serious recessions and other major economic shocks." *Id.*

> Promotes the safety and soundness of insured depository institutions and the U.S. financial system by identifying, monitoring and addressing risks to the deposit insurance funds. The FDIC also is the primary federal regulator of about 6,000 state-chartered "nonmember" banks (commercial and savings banks that are not members of the Federal Reserve System).141

"The heart of the FDIC's mission is to maintain stability and public confidence in the nation's banking and thrift systems."[142] "The FDIC sign-posted in insured financial institutions across the country has become a symbol of confidence."[143] "Today, the FDIC insures deposits of up to $100,000 in virtually all United States banks and savings associations."[144]

New technologies raise a wide range of supervisory issues. The FDIC does not desire to impose regulatory restrictions that can hinder the development of such emerging technology, but it does recognize the importance of providing guidelines for new products and services.[145] The FDIC has recognized the inherent risks of stored-value card systems, electronic banking in general, and Internet-based banks. These rapidly emerging banking activities on the Internet pose new questions regarding the scope of deposit insurance and its applicability to electronic funds. The purpose of federal deposit insurance is to maintain stability in the financial system and thus promote economic growth.[146] Deposit insurance also protects depositors from losses associated with bank failures and ensures the viability of smaller banks.[147]

One way to keep such confidence is by assuring consumers and merchants that funds are available for a transaction. For a deposit of funds to be recognized by the FDIC, it must qualify as a "deposit" under the Federal Deposit Insurance Act.[148]

---

141. *Symbol of Confidence*, *supra* note 140.

142. *Confidence for the Future*, *supra* note 140.

143. *Id.*

144. *Symbol of Confidence*, *supra* note 140.

145. Nicholas J. Ketcha, Jr., *Examination Guidance on the Safety and Soundness Aspects of Electronic Banking Activities-FDIC Financial Institution Letter FIL-14-97* (visited Feb. 26, 1997) <http://www.fdic.gov/banknews/fils/1997/fil9714.html> [hereinafter *FDIC Letter FIL-14-97*].

146. *Confidence for the Future*, *supra* note 140.

147. *Id.*

148. Under section 3(l) of the FDIA, "the term 'deposit' means"—

> (1) the unpaid balance of money or its equivalent received or held by a bank or savings association in the usual course of business and for which it has given or is obligated to give credit, either conditionally or unconditionally, to a commercial, checking, savings, time, or thrift account,

The FDIC published General Counsel Opinion No. 8 to address the issue of, "whether and to what extent the funds or obligations underlying stored value cards constitute 'deposits' within the meaning of section 3(l) of the Federal Deposit Insurance Act (FDIA) and are therefore assessable and qualify for deposit insurance."[149] General Counsel Opinion No. 8 identifies four types of stored value systems: 1) Bank Primary—Customer Account

---

or which is evidenced by its certificate of deposit, thrift certificate, investment certificate, certificate of indebtedness, or other similar name, or a check or draft drawn against a deposit account and certified by the bank or savings association, or a letter of credit or a traveler's check on which the bank or savings association is primarily liable: Provided, that, without limiting the generality of the term "money or its equivalent", any such account or instrument must be regarded as evidencing the receipt of the equivalent of money when credited or issued in exchange for checks or drafts or for a promissory note upon which the person obtaining any such credit or instrument is primarily or secondarily liable, or for a charge against a deposit account, or in settlement of checks, drafts, or other instruments forwarded to such bank or savings association for collection.

(2) trust funds as defined in this chapter received or held by such bank or savings association, whether held in the trust department or held or deposited in any other department of such bank or savings association.

(3) money received or held by a bank or savings association, or the credit given for money or its equivalent received or held by a bank or savings association, in the usual course of business for a special or specific purpose, regardless of the legal relationship thereby established, including without being limited to, escrow funds, funds held as security for an obligation due to the bank or savings association or others (including funds held as dealers reserves) or for securities loaned by the bank or savings association, funds deposited by a debtor to meet maturing obligations, funds deposited as advance payment on subscriptions to United States Government securities, funds held for distribution or purchase of securities, funds held to meet its acceptances or letters of credit, and withheld taxes: Provided, That there shall not be included funds which are received by the bank or savings association for immediate application to the reduction of an indebtedness to the receiving bank or savings association, or under condition that the receipt thereof immediately reduces or extinguishes such an indebtedness.

(4) outstanding draft (including advice or authorization to charge a bank's or a savings association's balance in another bank or savings association), cashier's check, money order, or other officer's check issued in the usual course of business for any purpose, including without being limited to those issued in payment for services, dividends, or purchases.

Federal Deposit Act, 12 U.S.C. § 1813(l)(1)–(4) (1994).

149. Federal Deposit Ins. Corp. General Counsel's Op. No. 8; Stored Value Cards, 61 Fed. Reg. 40,489, 40,490 (1996). *See also* Federal Deposit Act, 12 U.S.C. § 1813(l)(1)–(4) (1994).

Systems; 2) Bank Primary—Reserve Systems; 3) Bank Secondary—Advance Systems; and 4) Bank Secondary—Pre-Acquisition Systems.[150]

In the Bank Primary—Customer Account Systems, "funds underlying the stored value card could remain in a customer's account until the value is transferred to a merchant or other third party."[151] The merchant or third party then collects the funds from the customer's bank.[152] General Opinion No. 8 states that, "the funds underlying Bank Primary—Customer Account Systems [are] deposits under section 3(l)(1) of the FDIA, 12 U.S.C. 1813(l)(1)."[153]

In Bank Primary—Reserve Systems, a value is downloaded onto a card and funds are withdrawn from a customer's account or paid directly by the customer.[154] These funds are then paid into a reserve or general liability account at the financial institution to pay merchants or other payees as they make claims.[155] General Opinion No. 8 states that funds underlying Bank Primary—Reserve Account Systems are not "deposits" within the meaning of section 3(l)(1) of the FDIA.[156] The opinion stated that such funds are not credited to, or obligated to be credited to a commercial or thrift account.[157]

In Bank Secondary Systems,[158] the electronic value is created by a third party and the funds underlying the electronic value are ultimately held by such third party.[159] In such systems, depository institutions act as intermediaries in collecting funds from customers in exchange for electronic value. In Bank Secondary Systems, the electronic value is provided to the institution to have available for its customers. In Bank Secondary—Advance Systems, the customers exchange funds for electronic value while the funds are held for a short period of time and then forwarded to the third party.[160] General Opinion No. 8 states that funds underlying Bank Secondary—Advance Systems are not "deposits" within the meaning of section 3(l)(1) of the FDIA, because the liability is owed to the third party and the bank is

150. 61 Fed Reg. at 40,490 (1996).

151. *Id.*

152. *Id.*

153. *Id.* at 40,492; *see also* 12 U.S.C. § 1813(l)(1).

154. 61 Fed. Reg. at 40,494.

155. *Id.*

156. *Id.*; *see also* 12 U.S.C. § 1813(l)(1).

157. 61 Fed Reg. at 40,494.

158. In Bank Secondary Systems, the depository institution may have a contingent liability to redeem the electronic value from consumers and merchants. As such electronic value is redeemed, the institution may in turn exchange the electronic value for funds with the third party. *Id.*

159. *Id.*

160. *Id.*

holding the funds in the usual course of business.[161] However, if the funds are for a "specific purpose" and are held by the bank for a specific purpose, then the funds would be considered a deposit.[162]

In Bank Secondary—Pre-Acquisition Systems, the depository institution exchanges its own funds for electronic value from a third party, and then exchanges electronic value for funds with the bank's customers.[163] General Opinion No. 8 states that since the funds underlying Bank Secondary—Pre-Acquisition Systems are received and held by a third party and the depository institution, the funds are not "deposits" within the meaning of section 3(l)(1) of the FDIA.[164]

Regarding "electronic money," the FDIC is unwilling to recognize a deposit of funds underlying most stored value systems as a "deposit."[165] Not recognizing the funds as a "deposit" means that those merchants who use a stored value system are not assured that the transaction is properly funded and that they will be paid for their services or goods. Therefore, the merchants are reluctant to accept transactions using stored value systems, consumer confidence is jeopardized, and electronic commerce is hindered by using this type of electronic money system.

There are inherent risks with the emergence of electronic banking. One way the FDIC attempted to reduce those risks was by establishing electronic banking examination procedures. The examination procedures addressed the safety and soundness aspects, as well as associated risks of electronic banking.[166] The examination procedures were issued to FDIC examiners on January 29, 1997.[167] The FDIC produced guidelines as part of a comprehensive four-part approach to evaluating the wide range of risks that are inherent in electronic based activities. The first approach is the examination procedures with the remaining parts being: 1) a training program to educate FDIC examiners on how to use the examination procedures; 2) another set of procedures that address the technical aspects of electronic banking; and 3) a program to develop internal technical expertise.[168] The examination procedure included three levels of examination based on the sophistication of the institution's electronic

161. 12 U.S.C. § 1813(l)(1).

162. *Id.*

163. 61 Fed. Reg. at 40,494.

164. 12 U.S.C. § 1813(l)(1).

165. Federal Deposit Ins. Corp. General Counsel's Op. No. 8, *supra* note 149.

166. FEDERAL DEPOSIT INS. CORP., ELECTRONIC BANKING: SAFETY AND SOUNDNESS EXAMINATION FOR ELECTRONIC BANKING (Jun. 1998) [hereinafter SAFETY AND SOUNDNESS].

167. *FDIC Letter FIL-14-97*, *supra* note 145.

168. *Id.*

banking capabilities.[169] The examination procedures required an evaluation of six different areas of a bank's electronic banking capabilities.[170] The areas to be evaluated include the bank's planning efforts and implementation,[171] operating policies and procedures,[172] audit procedures,[173] legal and regulatory matters,[174] the bank's administration and system operations,[175] and vendors and outsourcing.[176] The FDIC's examination procedures, which the FDIC uses to review the worthiness of banking institutions for insurance coverage, contain key guidelines in maintaining the safety and soundness of the banking system.[177] These practices ensure that the electronic and conventional banking systems are secure and sound.

The FDIC is also addressing the risk associated with an Internet-based bank, or any institution that represents itself as a legitimate financial institution. The FDIC has recently launched a "Suspicious Internet Banking" web site to help detect potentially fraudulent Internet banking activity.[178] The web site provides the consumer and the industry a "user-

---

169. The three levels were: 1) information-only systems; 2) electronic information transfer systems; and 3) electronic payment systems. SAFETY AND SOUNDNESS, *supra* note 166, at 3.

> Level I systems can simply provide information as defined by the publisher or allow transmission of non-sensitive electronic mail (information-only systems); Level II systems can allow users to share sensitive information and communicate (electronic information transfer systems and Level III systems can facilitate electronic funds transfer and other financial transactions (electronic payment systems).

Id.

170. *Id.*

171. Planning and implementation risks include inadequate decision processes, system design and capabilities not meeting customer demands, increased competition with nonfinancial entities, and uncertain applicability of blanket bond/other insurance coverage to electronic activities. *Id* at 8.

172. Operating policies and procedures risks include managerial incompetence relative to electronic activities, and existing policies that may not address and control confidential electronic information and electronic channels. *Id.*

173. The internal control structure of the institution is critical to prevent, detect, and correct information security breaches. SAFETY AND SOUNDNESS, *supra* note 166, at 8.

174. Each system must be evaluated to determine its capability for initiating, completing, and enforcing legal documents and financial transactions. *Id* at 3.

175. Guidelines relating to access levels and record retention must be established and monitored on a regular basis. Efforts should be made to educate and support the consumers. *Id.*

176. Even if an institution outsources to a third party, the burden is still on management to supervise and control all aspects of the bank's systems. *Id.*

177. *Id.* at 13.

178. *Reporting Suspicious Internet Banking Sites* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/suspicious/sspcious.html>.

friendly" vehicle for reporting any entity that is misrepresenting itself as a federally insured depository institution.[179]

D. *The Office of the Comptroller of the Currency*

The Office of the Comptroller of the Currency ("OCC") charters, regulates, and supervises national banks to ensure a safe, sound, and competitive national banking system.[180] The OCC is an agency within the U.S. Department of the Treasury that continues to remove barriers in delivering banking services over the Internet.[181]

In the last several years, the OCC has continued to foster financial institutions delivering bank as well as nonbank services. In 1996, the OCC issued a bulletin that set forth guidelines relating to stored-value systems.[182] The bulletin not only describes different kinds of stored-value systems, but it also discusses risks associated with participating in stored-value systems.[183] The OCC approved the involvement of national banks in such stored-value systems as the Mondex system.[184] The Mondex system,[185] which is a smart card system, can transfer value from one card to another card.[186] The card uses a digital signature to authenticate a transaction.[187] It can also be used to make payments over the Internet. Mondex benefits consumers as well as merchants, because Mondex cash is easily reloadable and transferred, and

---

179. *Click on FDIC Web Site to Help Fend Off Fraudulent Internet Banks* (visited Dec. 25, 1998) <http://www.fdic.gov/consumer/consnews/sum98/fending.html>.

180. *Comptroller or the Currency Administrator of National Banks* (visited Feb. 20, 1999) <http:// www.occ.treas.gov>.

181. *See, e.g.*, OCC Guidance on Stored-Value Card Systems, O.C.C. Bulletin 96-48, 5 Fed. Banking L. Rep. (CCH) 49-971 (Sept. 10, 1996)) (source on file with author).

182. *Id.*

183. The OCC divides risks into three categories: 1) transaction risk, that includes the adequacy of internal controls, data integrity, transaction rules, employee performance, and operating processes; 2) strategic risk that includes business goals and strategies; and 3) reputation risk, that includes negative public opinion. *Id. See also OCC Issues Guidance on Smart Card/Stored Value Card Risks*, O.C.C. News Release 96-94 (Sept. 10, 1996).

184. Fisher-Haydis & Yancey, *supra* note 5, at 92.

185. The Mondex is a global electronic cash company formed by the U.K. based National Westminister Bank. USA TODAY, *Mondex Pitches New Way to Spend Money* (visited Dec. 17, 1998) <http://usatoday.com/money/wealth/consumer/mcw002.html>. Mondex is not technically money and it is not legal tender, because there is no requirement to accept it. *Id.*

186. All Mondex cards are considered to be little "purses" with independent stores of value. *Id.*

187. *Id.*

improves the efficiency at the point of sale.[188] The OCC recognized the issuance and redemption of electronic stored value as "functionally equivalent" or a "logical outgrowth" of the business of banking by a national bank.[189]

In 1997, the OCC approved the first virtual national bank charter.[190] Houston based CompuBank, N.A., was approved to deliver products and services to customers primarily through electronic means, and has applied to the FDIC for deposit insurance.[191] Such approval was in alignment with the OCC's decision to allow a national bank to provide electronic data interchange services, as well as electronic fund transfers.[192]

The OCC has recently issued bulletins that stress the importance of risk management in dealing with technology in general,[193] and especially with personal computer banking.[194] The guidance was put out to help the estimated 2600 national banks that engage in some form of personal computer banking.[195] The OCC identified online transactions as the most common source of risk that includes unauthorized interceptions, data alteration, system failures, and computer viruses.[196] The OCC recommends that national banks implement risk management practices that establish policies and procedures, internal controls, and system monitoring.[197] To assist in this effort, the OCC issued guidelines for examiners to follow when

188. *Id.* Making a payment through Mondex takes less than three seconds to complete and the payments are exact. USA TODAY, *supra* note 185. Mondex also reduces the security risks of storing and transporting currency. *Id.* It can even "hold up to five different currencies." *An Overview of Mondex* (visited Jan. 14, 1999) <http://www.amdahl.com/doc/products/smartcard/overview.html>.

189. In evaluating whether the proposed activity was within the "business of banking," the OCC evaluated: 1) whether the activity was "'functionally equivalent' to or a 'logical outgrowth' of a recognized banking activity; 2) whether the activity would 'respond to customer needs or otherwise benefit the bank or its customers;' and 3) whether the activity 'involve[s] risks similar in nature to those already assumed by banks.'" Wilson, *supra* note 14, at 714.

190. *OCC Says OK to First Virtual National Bank Charter*, 16 No. 18 BANKING POL'Y REP. 6, 6 (Sept. 1997) (source on file with author).

191. *Id.*

192. The OCC revised 12 C.F.R. part 7 to include the "activities, functions, products and services provided by banks via electronic means and facilities." 12 C.F.R. § 7.1019 (1998). Prior to the revision, 12 C.F.R. part 7 authorized banks to utilize data processing equipment to analyze financial data for itself and others. *See* 61 Fed. Reg. 4,853 (1996) (codified at 12 CFR § 7.1019 (1998)).

193. *Id.*

194. *OCC Banking Bulletin No. 98-38* (visited Jan. 18, 1999) <http://www.occ.treas.gov/ftp/bulletin/98-38.txt>.

195. *Id.*

196. *Id.*

197. *Id.*

reviewing a bank's technology risk management procedures.[198] The Technology Risk Management guidance is one of the agency's most comprehensive statements on technology issues that provides national banks and examiners with a framework for managing technology as a vital part of the bank's services. The OCC encourages security policies, awareness, and controls that result in reliable access control, user authentication, data integrity, data privacy, and transaction verification.[199] The guidance also suggests system "firewalls" to prevent system penetration.[200] Examiners will evaluate senior management regarding sufficient knowledge and skills, as well as their planning process to manage technology-related risks.[201]

The bulletin also addresses using third party personal computer systems. The bulletin stresses the need to manage and review the third party's financial conditions, its internal control practices, and rights if the third party system should fail.[202] Finally the OCC encourages all national banks to keep abreast of new developments in electronic banking.[203] Such monitoring should include both state and federal changes and implementation of rules and regulations.[204]

The OCC recognizes the importance of the banking industry's showing of leadership in advancements in electronic banking. At the beginning of 1998, the OCC approved the application of a Utah Bank, Zions First National Bank, to be the first financial institution to offer digital signature products to its customers.[205] It has also been working to address consumer concerns by analyzing findings by such groups as the Consumer Electronic Payments Task Force which the Treasury Secretary asked the OCC to chair in 1996.[206] Such findings show that consumers want adequate disclosure about a company and less disclosure about themselves. At the same time, the

---

198. *See OCC Warns Banks on Technology Risks* (visited Dec. 25, 1998) <http://www.occ.treas.gov/ftp/release/98-13.txt> [hereinafter *OCC Warns*].

199. *Id.*

200. *Id.*

201. These risks include risks associated with computer hardware, software applications, and telecommunications services. *Id.* The risks fall into four categories: transactions, strategic, reputation, and compliance risks. *Id.*

202. *OCC Warns*, *supra* note 198.

203. *Id.*

204. *Id.*

205. *OCC Approves a National Bank to Certify Digital Signatures* (visited Dec. 22, 1998) <http://www.occ.treas.gov/ftp/release/984.htm>. Digital signatures are used for electronic authentication of the sender of an electronic message. *Id.* As stated by Comptroller of the Currency, Eugene Ludwig, "The ability to verify and authenticate electronic signatures is essential to the development of electronic commerce and electronic banking." *Id.* The Utah bank plans to focus on certification services involving corporate and government documents. *Id.*

206. *See Consumer Electronic Payment Task Force* <http://www.occ.treas.gov/>.

OCC has recognized the need for limiting government restrictions and providing predictable government involvement whenever it is necessary.[207] The OCC, through its broad range of banking policies, is promoting self-regulation and is diligently working to show that public concerns about privacy and disclosure of information can be addressed without requiring externally imposed government solutions.[208]

V. ELECTRONIC MONEY AND BANK RELATED ISSUES

A. *Nonbank Institutions as Financial Providers*

There are many types of financial institutions, including federal and state chartered depository institutions, check-cashing organizations, insurance companies, and brokerage firms.[209] All of these institutions are subject to extensive state and federal regulations to protect the integrity of our monetary system. The dilemma is that if nonbank entities are not classified and regulated as banks, but are allowed to provide limited bank-like services put our monetary system is at risk because it is through regulation that federal agencies protect the consumer and the United States financial system. Part of the problem is that the federal banking regulations do not provide a consistent definition of the term "bank." For example, the Bank Holding Company Act defines a "bank" as any FDIC insured bank or any institution that accepts demand deposits and engages in the business of making commercial loans.[210] Under the Federal Deposit Insurance Act, a "bank" includes an institution chartered as a bank or any other "banking" institution that is engaged in the business of receiving deposits.[211] Under the National Bank Act, core "banking" functions generally include the receiving of deposits, paying checks, and making loans.[212] If a standard definition is established, the issue then becomes whether nonbank entities qualify as a "bank" and should be required to meet banking regulations.

---

207. Julie L. Williams, *Remarks at the Banking Roundtable Lawyers Council, Washington, D.C.* (May 8, 1995) (visited Dec. 22, 1998) <http://www.occ.treas.gov/ftp/release/98-2d50a.txt.>.

208. *Id.*

209. Wilson, *supra* note 14, at 671.

210. Melanie L. Fein, *In Cyberbanking, When Do Non-Banks Become 'Banks'?*, 15 No. 5 BANKING POL'Y REP. 10, 10 (1996).

211. *Id.*

212. *Id.*

A number of nonbank entities currently offer a variety of bank-like services, including issuing and providing new electronic payment products such as stored value cards and digital cash.[213] Nonbank institutions have the potential to be high-risk operations which regulation must address in order to provide the consumer confidence and safety that traditional banking institutions provide to their customers. Many of these nonbank entities are using electronic money to provide different types of services. Again, DigiCash and CyberCash Inc., have developed Internet payment systems and are continuing to establish a trusted link between the Internet and banks.[214] Therefore, it is likely that nonbank entities will issue electronic value in exchange for United States currency. This situation generates two important questions: 1) Where is the U.S. currency stored that is exchanged for electronic value?; and 2) Is the U.S. currency insured while it is stored?

Just recently, the importance of these questions came into focus when DigiCash filed for bankruptcy protection under Chapter 11.[215] A traditional bank would have FDIC insurance. Currently, any currency held by a nonbank such as DigiCash is not insured by the FDIC and the nonbank retains control over it under a Chapter 11 ruling. Such a situation places our monetary system at risk and would have a negative impact on the growth of electronic commerce and Internet banking, because a lack of consumer confidence is fostered.

Under the current structure, the entity would have to qualify as a bank before federal banking regulators could examine and control the activities of the issuer.[216] As mentioned previously, the FDIC does not treat the funds stored in value cards as deposits and there is currently no indication that the FDIC will insure nonbank entities.[217] In addition, electronic money is yet to be considered legal tender.[218] Assuming the entities issuing smart cards and other electronic value do not qualify as banks, and are not covered by our federal banking regulations, then the question remains whether the bank

213. *See generally Digicash* (visited Jan. 14, 1999) <http://www.digicash.com/digicash/digicash/profile/index.html>.

214. *CyberCash - Free Wallet* (visited May 10, 1998) <http://www.cybercash.com/cybercash/consumers/wallet.html>.

215. *Welcome to DigiCash* (visited Jan. 14, 1999) <http://www.digicash.com/digicash/index.html>.

216. Federal Deposit Act, 12 U.S.C. § 1813 (1994).

217. 12 U.S.C. § 1813(3)(l) (Supp. 1997).

218. *Id. See also* Federal Deposit Ins. Corp., General Counsel's Op. No. 8; Stored Value Cards, 61 Fed. Reg. at 40,490 (1996).

regulatory agencies should extend their governance over such entities, or if some other form of governmental intervention is needed to regulate them.

With these institutions using "electronic money," it is imperative that such nonbanks be regulated and be required to adhere to the same standards as a bank. If electronic money is to become equivalent to legal tender, then it must also be as secure as money is today. Nonbank institutions providing such money and services must rise to the same standards as banks and provide the same level of consumer protection.

B. *Privacy Issues*

There are a number of privacy issues that arise for the financial institutions and the consumers. One issue is whether electronic banking services that are processed through the Internet compound the possibility of confidential account information being obtained or tampered with by third parties.[219] Another issue is the potential disclosure of personal information to third parties due to the consumer's unfamiliarity with new banking products.[220] The financial system relies on current privacy legislation to define the limits of a third party's legal right to access a person's financial information. However, current privacy legislation does not address the heightened privacy concerns raised by the use of electronic money on the Internet.[221] Current legislation includes the Privacy Act of 1974 ("Privacy Act"),[222] the Right to Financial Privacy Act of 1982 ("RFPA"),[223] and the Electronic Communications Privacy Act of 1986 ("ECPA").[224]

The Privacy Act protects an individual's private information, regulates the practices of federal agencies regarding personal information, and balances the individual's need for privacy and the government's need for such information to fulfill certain functions.[225] Each federal agency must

---

219. Robert G. Ballen & Thomas Fox, *The New Business of Banking: What Banks Can Do Now: Legal Issues in the New World of Cyberbanking*, 912 PRAC. LAW. INST. CORP. L. HANDBOOK SERIES 497, 503–4 (1995).

220. *Id.*

221. Catherine M. Downey, *The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?*, 14 J. MARSHALL J. COMPUTER & INFO. L. 303, 308 (1996).

222. In 1974, Congress enacted the Privacy Act, which was the first federal statute recognizing the need to balance an individual's concern for information privacy with the institutional practice of storing information in a computerized record-keeping system. 5 U.S.C. § 552(a) (1974).

223. 12 U.S.C. § 3402 (1982).

224. 18 U.S.C. § 2510 (1986).

225. H.R. REP. No. 95-1383 at 33–34 (1978).

register the existence of every federal data bank in the Federal Register.[226] Furthermore, no federal agency may disclose any record contained in its system to any other person or agency without the written request or consent of the individual.[227]

In 1982, Congress enacted the RFPA to further protect customer financial records.[228] Under the RFPA no government authority may have access to, or obtain copies of, information contained in the financial records of any customer from a financial institution, unless the customer authorizes such disclosure.[229]

The ECPA[230] protects the individual against the interception of electronic communications by an unauthorized person. Titles I and III of the ECPA pertain to common computer-to-computer communications, including the transmission of financial records or funds transfers among financial institutions.[231] Title I focuses on electronic communications, and thus directly applies to most of the data exchanged between parties using the Internet.[232] Title II states that a communications service provider "shall not knowingly divulge the contents of a communication" while in electronic storage when communications arrive electronically, and the service provider retains records solely for processing and storage.[233]

However, the potential for intrusions by unauthorized persons and exposure of a user's financial information is still possible on the Internet, which is beyond the protection of the ECPA. Without adequate privacy protections, transactions conducted on the Internet can be exposed to third parties. One solution is increased usage of encryption.[234] It can be argued that without encryption there will be widespread invasion of privacy, and increased criminal activity. Also, it can be argued that because consumers may not be familiar with the potential disclosure of personal information to

---

226. 5 U.S.C.A. § 552(a) (1998).

227. *Id.* at 3. However, there are several exceptions to the Privacy Act through which federal agencies can gain access to an individual's record to combat criminal activity. *Id.*

228. 12 U.S.C. § 3402 (1998). Furthermore, the Privacy Act allows an individual to copy, correct, and challenge his personal information stored in the data banks of the federal agencies. *Id.*

229. *Id.* In order to obtain a customer's financial records from a financial institution, the federal government must follow the procedural requirements of the RFPA and submit a written certification indicating its compliance. *Id.* However, the customer faces difficult obstacles in challenging or blocking the disclosure of his financial records, and must usually wait until after such disclosure to dispute the government's intrusion. *Id.*

230. 18 U.S.C. §§ 2510–18 (1994).

231. *Id.*

232. *Id.*

233. *Id.* § 2511(3)(a) (1994).

234. *See infra* text accompanying note 254.

third parties, regulatory agencies must take affirmative steps to protect the consumer.[235]

C. *Security Risks*

The Internet is "inherently insecure,"[236] and the typical person using the Internet is unaware of the risk, since a large portion of today's activities on the Internet is based on information retrieval. However, financial institutions face the difficulty of processing transactions in this same environment. Transactions occurring on the Internet are over a public network that is open and available to anyone, including criminals. A knowledgeable person could trap, change, and redirect information and transactions that occur on the Internet. The average person could not perform this type of criminal act because it takes special knowledge, software, and hardware tools to do so, but the number of people with these skills is growing every day. A cyber criminal may transfer funds into another account, make unauthorized purchases, or even obtain money from others. With voluminous transmissions and open travel over the Internet, all data transfers potentially can be read or monitored by a third party. In particular, there are "sniffer" systems that are available to anyone, that can be set up on any network at any port that look for and collect certain types of data.[237] While these systems are legitimately used in network management, the systems can also be used in illegitimate activities such as theft of credit card numbers or passwords.

Any connected data storage systems, and any data stored on an Internet server may be susceptible to compromise, if proper security precautions are not taken. Data integrity is also in jeopardy because the Internet can potentially allow those with specific knowledge and tools to alter or modify data during transmission.[238] There are other security risks associated with banking on the Internet. These include risks associated with authentication, non-repudiation, and access control.[239]

It is essential to be able to verify that a particular communication, transaction, or access request is legitimate and accurate.[240] This verification

235. Ballen & Fox, *supra* note 219 at 503.

236. FDIC, Division of Supervision FIL-131-97: *Security Risks Associated with the Internet* (Dec. 1997) <http://www.fdic.gov/banknews/fils/1997/fil97131.html> [hereinafter *Security Risks*].

237. *Id.*

238. *Id.*

239. *Id.*

240. *Id.*

process is known as authentication.[241] "[A] computer system . . . on the Internet is identified by an Internet Protocol ("IP") address which works [much like] a telephone . . . number."[242] The key difference is that this number is set dynamically each time a user connects to the Internet.[243] Because it is dynamically set, the physical destination and origin of transactions are difficult to verify or authenticate using conventional methods.[244] Thus, the door opens for any person to intercept or pose as someone else on the Internet. An intruder can use a technique called "spoofing"[245] to gain access to the system and pose as an authorized user, or can use a software program that generate passwords from the information gathered from an unauthorized access to a program.[246] Because of these possible interceptions, authentication controls are necessary to identify all parties to a communication.

Nonrepudiation is essential for validating data.[247] "Nonrepudiation involves creating proof of the origin or delivery of data to protect the sender against the recipient denying that the data has been received or to protect the recipient against false denial by the sender that the data has been sent."[248] Therefore, "to ensure that a transaction is enforceable, steps must be taken to prohibit parties from disputing the validity of, or refusing to acknowledge, legitimate communications or transactions."[249]

Risks associated with access control of systems must also be addressed by a financial institution. Access control refers to protecting the integrity of the network and its supporting systems from unauthorized access by using the most innovative software and hardware technology available.[250] "Risks include the destruction, altering, or theft of data or funds; compromised data confidentiality; denial of service (system failures); a damaged public image; and resulting legal implications."[251] Constant monitoring of the system is required because hackers, unscrupulous vendors, former or disgruntled employees, or even agents of espionage may try to invade the system.[252]

---

241. *See also Security Risks, supra* note 236; Randy V. Sabett, *Cryptography, Smart Cards, and Future Banking technology* (visited Jan. 1, 1999) <http://venable.com/litlab/eblcr5.html>.

242. *Security Risks, supra* note 236.

243. *Id.*

244. *Id.*

245. *Id.* "IP spoofing" is to have one computer set up to act as another computer. *Id.*

246. *Security Risks, supra* note 236.

247. *Id.*

248. *Id.*

249. *Id.*

250. *Id.*

251. *Security Risks, supra* note 236.

252. *Id.*

Once an intruder has gained access, they could change advertised rates on financial transactions or possibly even shut down an entire system. As we work to protect the integrity of the Internet and this new emerging banking system, there are intruders working to take advantage of whatever weaknesses there are in the network. There are software programs that run security scans on Internet servers, firewalls, and internal networks, which can help an intruder identify and attack a system by finding its weak link.[253] Because of the security risks described above, a financial institution should implement several security measures that are presently available.

One such security measure is encryption.[254] Encryption, or cryptography, is a method of converting information to an unintelligible piece of data and then, through decryption, changing it back to its original understandable form.[255] "The information is encrypted (encoded) and decrypted (decoded) by . . . 'cryptographic keys.'"[256] The encryption renders the information unreadable because it appears as a series of unorganized characters. Thus, the encryption technology provides assurance of data privacy, confidentiality, and integrity, with some methods providing protection against forgery and tampering.

There are symmetric and asymmetric cryptographic key systems. "With a symmetric key system (also known as secret key or private key system), all parties have the same key" to encrypt and decrypt messages.[257] The distribution of a key to each party in a transaction over a large network is impractical for widespread use. In an asymmetric key system (also known as a public key system), there are two keys, with one being secret (a "private key") and one being public (a "public key").[258] The private and public keys are mathematically related so that the corresponding public key can only decrypt the private key. Similarly, the corresponding private key that is specific to a party or computer system can only decrypt the public key. This system, therefore, authenticates the private key holder. More importantly, "it is nearly mathematically impossible for the holder of any public key to use it to figure out what" or who holds the private key.[259] The strength of the key is

253. *Id.*

254. *Id.* "Encryption techniques directly address the security issues surrounding data privacy, confidentiality, and data integrity. Encryption technology is also employed in digital signature processes, which address the issues of authentication and non-repudiation." *Id.*

255. *Security Risks*, *supra* note 236.

256. *Id.* "These 'keys' are actually values, used by a mathematical algorithm to transform the data. The effectiveness of encryption technology is determined by the strength of the algorithm, the length of the key, and the appropriateness of the encryption system selected." *Id.*

257. *Id.*

258. *Id.*

259. *Security Risks*, *supra* note 236.

determined by the length of the key. Therefore, a longer key makes it harder for high-speed computers to break the code.[260]

A digital signature is another type of cryptography that can be used as a security measure by a financial institution. Digital signatures authenticate the identity of the sender by using the private key.[261] The digital signature is derived from the content of the message itself, establishing a link such that the message cannot be repudiated.[262] "To generate a digital signature, the original, unencrypted message is run through a mathematical algorithm that generates what is known as a message digest."[263] "The message digest is then encrypted with a private key, and sent along with the message."[264] The recipient decrypts the message digest, and if the resulting message digest matches the one sent with the message, the message has not been altered.[265] Thus, data integrity has been verified. Because the message digest was encrypted with a private key, the sender can be identified and connected to the specific message and the digital signature cannot be reused.[266]

"Certificate Authorities" and digital certificates are other ways to address security concerns, particularly in the area of authentication. "A 'Certificate Authority' is a trusted third party that verifies the identity of a party to a transaction."[267] The identities of all parties must have been proven to the "Certificate Authority" beforehand. Digital certificates are messages that are signed with the "Certificate Authority's" private key.[268]

An individual bank's activities will dictate the level and type of security measures required. This may, for instance, include encryption, digital signatures, certificate authorities, and digital certificates.[269] With technology and implementation standards changing daily, the necessary legal infrastructure will continue to evolve and possibly lead to further regulation.

In November 1997, the Electronic Financial Services Efficiency Act of 1997 ("Act") was introduced, granting legal validity and equal treatment to qualifying forms of electronic authentication.[270] Any form of electronic

---

260. *Id.*

261. *Id.*

262. *Id.*

263. *Id.* A message digest is a unique character representation of the data. *Security Risks, supra* note 236. This process is known as the "hash." *Id.*

264. *Id.*

265. *Id.*

266. *Id.*

267. *Security Risks, supra* note 236.

268. *Id.*

269. *Id.*

270. *Id. 21st Century Banking Alert, No. 97-11-13* (visited Jan. 29, 1998) <http://www.fflisj.com/bancmail/21starch/ 971113.html> [hereinafter *21st Century Banking*]. House Report

authentication would be valid and legal according to this Act, if it "reliably establishes" both the identity of the maker, sender, or originator of a document, communication, or transaction and the fact that the document, communication, or transaction, has not been altered.[271] Therefore, any record would be valid and legal according to the Act with a qualified electronic authentication, unless state law prohibited it.[272] For the authentication to be valid, it must be:

> (i) unique to the person making, sending, or originating a document or communication;
>
> (ii) capable of verification;
>
> (iii) under the sole control of the person using it; and
>
> (iv) linked to data or a communication transmitted in such a manner that if such data or communication has been altered, the authentication becomes invalid.[273]

In particular, the Act authorizes that a digital signature, accompanied by a certificate issued by a third party, can be used in lieu of a paper based written signature in any communication that requires a signature within a federal agency, a United States court, or other instrument of the United States government.[274] The Act also established a National Association of Certification Authorities ("NACA") as the central association with which any person or group must register, in order to qualify as an authentication service provider.[275] Despite movement toward providing authentication standards, the Act does leave some issues unresolved, including the liability of the certification provider and the role of NACA. This emerging technology, while providing additional security for financial institutions, is still in its infancy, during which many new developments and regulations will surface.

2937, the Electronic Financial Services Efficiency Act of 1997, was introduced by Representatives Richard H. Baker (R-LA) and David Drier (R-CA). *Id.*

271. *Id.*

272. *Id.* A significant number of states have enacted or are considering enacting digital signature or other electronic authentication laws. *Id.*

273. *21st Century Banking*, *supra* note 270.

274. *Id.*

275. *Id.*

D. *Consumer Protection*

1. Regulation E and the Electronic Funds Transfer Act

Regulatory agencies are expected to provide the financial structure that protects the average consumer as well as the financial systems. However, in order for this to work, banks must comply with these regulations. Regardless of whether a bank uses a third party provider for Internet banking services, it must comply with applicable federal and state laws and regulations when it comes to consumer protection.[276] These regulations help provide consumer protection and confidence. Many consumer protection laws regarding wire transfers come from the Electronic Fund Transfers Act of 1978 ("EFTA").[277] The Federal Reserve Board promulgated Regulation E ("Regulation E") to implement the EFTA.[278] Regulation E covers all electronic funds transfers ("EFT").[279] Both the EFTA and Regulation E are consumer protection laws that amount to a "consumer bill of rights" in electronic banking.[280] The EFTA and Regulation E provide for consumer protection through disclosures, liability limits, documentation, and error resolution procedures.[281] The EFTA and Regulation E require that: 1) consumers are given an initial and periodic disclosure statements of the terms and conditions of the electronic funds transfer service; 2) there are safeguards with respect to pre-authorized debits and credits; 3) limitations are imposed on consumer liability for unauthorized use of credit and banking services; and 4) financial institutions investigate and resolve billing errors through error resolution procedures.[282]

On May 2, 1996, the Federal Reserve Board issued a proposed rule for the application of Regulation E to stored value systems.[283] Applying

---

276. Dan C. Aardal, *Consumer Protection Issues in Home Banking, Electronic Banking Developments: U.C.C. and Selected Regulatory Perspectives*, 1996 ABA SEC. BUS. L. at 25, 31 (1996).

277. 15 U.S.C. § 1693 (1994).

278. Electronic Fund Transfers, 12 C.F.R. § 205 (1998).

279. An electronic funds transfer ("EFT") is defined as "any transfer of funds that is initiated through electronic, terminal, telephone, or computer or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit an account." *See* 12 C.F.R. § 205.3(b); *see generally* Michael A. Fixler, *Cyberfinance: Regulating Banking on the Internet*, 47 CASE W. RES. L. REV. 81, 90 (1996).

280. Aardal, *supra* note 276, at 31.

281. *Fed Study Recommends Alternatives to Reg E for Stored-Value Cards*, 16 No. 8 BANKING POL'Y REP. 13, 15 (1997).

282. Barbara E. Matthews, *Reg E and Stored Value Cards: Fed is on Right Track*, 15 No. 14 BANKING POL'Y REP. 4 (1996). *See also* Aardal, *supra* note 276, at 1–2.

283. *Id.*

Regulation E to electronic money, especially through stored value systems, has the potential of interfering with the use of electronic money, but it also provides consumers with certain protections whenever a consumer's account is accessed electronically. The proposed rule focused on the type of stored value system rather than the entity issuing the card.[284] The Federal Reserve Board divided stored value systems into three types: "online accountable," "offline accountable," and "offline unaccountable."[285] Online accountable system is a system that only requests a transfer at the bank's central database.[286] These systems were deemed to be subject to Regulation E with modification for the particular nature of the system. Whereas offline accountable system is one in which the transactions took place offline but the bank had the ability to determine the impact of the transaction on the customer's balance.[287] The offline accountable systems have been regarded as being minimally regulated, with the focus turning to adequate disclosure to consumers. The third type identified was the offline unaccountable system which are those systems in which the transaction took place offline and there is no central database at the bank.[288] This type of system is deemed to be not regulated by Regulation E. The proposed rule outlining these types of stored value systems were the first steps toward providing consumer protection for electronic transactions. Such efforts will foster the application of existing or creation of new consumer protection laws for banking on the internet.[289]

2. Consumer versus Bank Liability

The question of consumer liability for unauthorized transfers was debated in Congress and resulted in a compromise between banks and

---

284. *Id.*

285. *Id.*

286. John L. Douglas, *Electronic Money*, 17th Annual Corporate Counsel Institute (unpublished) December 10, 1998. Online accountable systems were those systems where the bank retained an account in the name of the customer, which was debited only when the information related to the transaction was noted by the bank. *See generally* Richard L. Field, *1996: Survey of the Year's Developments in Electronic Cash Law and the Law Affecting Electronic Banking in the United State*, 46 AM. U. L. REV. 967, 976 (1997).

287. For an online accountable system, there is no authentication or authorization for the transaction but there is still a central database that records values and keeps those transactions apart from the card. *See generally* Field, *supra* note 286.

288. *Id.* The system allows for the stored value card involved to be used independently when there is no centralized bank that maintains all the transactional information. *Id.* In other words, the transactional information and reconciliation of the transactions occur on the card. *Id.*

289. 12 C.F.R. § 205.6(b) (1998).

consumer groups' positions.[290] An unauthorized transfer is a transfer initiated by someone other than the customer and without actual authority from the customer.[291] The banks supported a "negligence" standard in which a consumer has no liability unless the consumer's negligence contributed to the loss.[292] Consumer groups pushed for a flat fifty dollars liability limit similar to the limit imposed for credit card fraud.[293] Section 909 of the EFTA and Section 205.6 of Regulation E represent the compromise of these two groups by holding consumers liable for "unauthorized" electronic fund transfers, but that liability is sharply limited.[294] Aside from two exceptions, a consumer's liability for an unauthorized transfer is limited to the lesser of fifty dollars or the amount obtained in the unauthorized transfer.[295] However, a consumer is held liable for unauthorized transfers which resulted from the consumer's own negligence.[296]

Another area in which there are limits on consumer liability is in an unauthorized transfer from a breach of home banking security.[297] For example, a "hacker"[298] can break into a database containing access card numbers and personal identification numbers, which are maintained by the bank or a third party service provider, and use them to make transfers. Also a consumer may transmit a transaction from home to the bank and the transaction is intercepted by an unsuspected third party. In such situations, analysis of the EFTA and Regulation E would suggest that the bank will be held liable.[299] Such breach of security constitutes unauthorized electronic fund transfer in which the customer has limited liability. Therefore, with the prospect of being liable for breaches of system security, it is imperative that

---

290. *See generally* Aardal, *supra* note 276.

291. *Id.* § 12 C.F.R. 205.2(m) (1998). An unauthorized transfer is defined in Section 205.2(1) of Regulation E. *Id.* 12 C.F.R. § 205.2(l). If a transfer is performed by someone who is not authorized then the customer has limited liability. *Id.*

292. *Id.* § 205.6(a).

293. *Id.* § 205.6(b).

294. Aardal, *supra* note 276, at 32.

295. *Id.*

296. *Id.* at 33. Such negligence includes safeguarding a Personal Identification Number (PIN). *Id.* at 34. Therefore, a bank can highly recommend that a customer safeguard a PIN but can not hold that consumer liable if the consumer writes that PIN on the top of the access card. *Id.*

297. Aardal, *supra* note 276, at 35.

298. A hacker is somebody who knows the ins and outs of an operating system, a network, or computer language. A "bad" hacker defaces web sites with electronic graffiti, or steals user names, passwords or credit card numbers from an operating system or network. Adam L. Penenberg, *Forbes Digital Tool: Entertainment – Hacking the Corporate Ladder* (visited Feb. 17, 1999) <http://www.forbes.com/tool/html/97/oct/1010/feat.htm>.

299. Aardal, *supra* note 276, at 35.

banks focus on security issues at all levels. The bank has the burden of proving that the transaction was authorized.[300] The consumer then can point out that the bank should bear liability for breaches of security, since it was the bank who selected the computer program, the mode of telecommunications, the third party service providers who may be involved, and the components of the home banking system.[301] Thus, it becomes important that the bank have strong agreements with home banking service providers, processors, software vendors or developers to limit the bank's liability due to failures attributable to third parties.[302]

A consumer is also protected from a bank's failure to make an electronic fund transfer through section 910 of the EFTA. Section 910 of the EFTA protects the consumer by holding that the bank is liable for the failure to make an electronic fund transfer and for all damages proximately caused by such failure to make such a transfer.[303] Shifting liability to the bank is crucial in developing consumer confidence in using electronic payment systems and performing banking transactions over the Internet.

VI. CONCLUSION

Entering the new millenium, the Internet has become a remarkable convergence of break through technology for numerous information-based and monetary-based industries such as banking. A whole new arena of electronic commerce is emerging, which is reshaping and revolutionizing our banking practices. As the printing press, the automobile, the telephone, and the airplane brought the world together, so is the Internet transcending borders. But, with advancement comes difficult strategic choices in determining the path of a system as open as the Internet without hindering progress. It is within this medium that regulatory agencies must become leaders in setting precedent in dealing with the challenges of privacy, security, and jurisdictional issues. Banks have gained the confidence of the consumer in the past. The challenge now is to gain that some level of consumer confidence in banking on the Internet. Therefore, it is vital that regulations and standards dealing with security measures, such as encryption and digital signatures, continue to evolve. Banks are faced with many

300. Section 909(b) of the EFTA places the burden of proving such a transaction was authorized on the bank. *Id.* at 36.

301. *Id.*

302. *See* Wilson, *supra* note 1, at 33.

303. *Id.* A bank is liable to a consumer for all damages proximately caused by the bank's failure to make an electronic fund transfer in the correct amount or in a timely manner or due to insufficient funds that resulted from such failure to transfer such funds. *See* Aardal, *supra* note 276, at 36.

challenges, including the emergence of electronic money and criminals on the Internet. Also, the lines between a traditional financial institution such as a bank and nonfinancial institutions are becoming blurred, and banks are now competing for the consumer's business. All these changes reflect the impact of the Internet on our banking practices.

It is very necessary to establish a strategy and a roadmap for electronic banking. Banking, unlike the remainder of electronic commerce, is a highly regulated industry. It is important that nonbank entities fall under a formal regulatory structure. With this structure two key items can occur. First, a uniform set of enforceable regulations on banking worthiness can be established. This will enhance customer confidence. Second, a strategic plan can be developed on a global level by the G-10 and its member nations, that can use the decades of banking experience to steer the new inexperienced electronic banking industry away from potential pitfalls and banking failures. It is good to remember what happened on October 17, 1987 ("Black Monday"). Part of the failure in the stock market was caused by an uncontrolled "programmed sell-off."[304] If regulations are not established for all types of Internet banking, both banks and nonbanks will be open to the same type of mass electronic flooding of systems, or an electronic "run" on banks. A bank could be out of business in a matter of hours.

Together the private and public sectors can establish a new electronic banking and commerce environment that will enable new opportunities to promote growth of and expand our world economy by reaching new customers, lowering operating costs, and extending financial institutions and nonfinancial institutions to new levels of service, delivery, and innovation.

Jacqueline Marcucci

304. CNNfn - *The blackest of Mondays – Oct. 13, 1997* (visited Feb. 6, 1999) <http://cnnfn.com/markets/9710/13/crash_main/>.