1996

A Call for International Legal Standards for Emerging Retail Electronic Payment Systems

Sarah Jane Hughes
Indiana University Maurer School of Law, sjhughes@indiana.edu

A CALL FOR INTERNATIONAL LEGAL STANDARDS FOR EMERGING RETAIL ELECTRONIC PAYMENT SYSTEMS

SARAH JANE HUGHES*

I. INTRODUCTION

The announcement of Internet-based and other new retail electronic payments mechanisms,[1] one of the biggest changes in banking in the recent past, may threaten traditional notions of what constitutes "the business

---

*Adjunct Associate Professor of Law at Indiana University-Bloomington. Fred Cate, Jeffery Atik, Robert Kaiman, and Elinor Harris Solomon provided helpful comments and criticisms. I am grateful for the research assistance of former and current students, Lori Yarbor, Christopher Goff, and Michael Vreeland. Despite so much help, all responsibility for errors that may appear is mine.

[1]"Retail electronic payment systems" offer equivalents of cash or certain retail banking transactions—particularly checks, drafts, and other credit or debit transfers—primarily in support of purchase transactions. *See* David Laster & John Wenninger, Policy Issues Raised by Electronic Money, paper prepared for the Columbia Institute for Tele-Information's Conference on Digital Cash and Electronic Money, 1-2 (April 21, 1995) (copy available on file with the author) (describing the potential for electronic payments to displace "physical currency, checks, and credit card transactions"). These systems are similar to "financial electronic data interchange" services in that they combine electronic transfers of funds and of remittance data. *See* Scott Knudson et al., Business-to-Business Payments and the Role of Financial Electronic Data Interchange, 80 Fed. Res. Bull. 269 (April, 1994) (illustrating how electronic data interchange in standard formats has allowed business trading partners to replace labor intensive activities such as issuing, mailing, and collecting checks through the banking system with automated initiation, transmission and processing of payment instructions).

of banking."[2] At the very least, new electronic payments mechanisms challenge traditional "banking" activities such as holding deposits, clearing checks, conducting foreign exchange, and executing wholesale wire transfers over bank-based funds transfer networks. Indeed, these new payments options appear poised to eliminate many "banking" functions from the province of banks and other financial intermediaries with which bank customers customarily deal.

Viewed most favorably, emerging retail electronic payments mechanisms offer enormous opportunities for efficient financial services and commerce. Viewed least favorably, they create opportunities for serious mischief such as penetrations of major banks' computer systems,[3] fraudulent investment offers,[4] speedy and anonymous means of laundering drug profits,[5] on-line gambling,[6] and threats to the exercise of national monetary policy.[7] In addi-

---

[2]12 U.S.C. § 24(Seventh) (1994) (The National Bank Act of 1863, as amended); U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, U.S. BANKS AND INTERNATIONAL TELECOMMUNICATIONS 2, OTA-BP-TCT-100 (1992) [hereinafter 1992 OTA PAPER].

[3]Kelley Holland, *Bank Fraud, the Old-Fashioned Way*, BUS. WK., Sept. 4, 1995, at 96 (describing how youth in St. Petersburg, Russia allegedly penetrated and siphoned off $400,000 from Citibank's cash management accounts and attempted to steal more than $10 million more); *Policing Cyberspace*, U.S. NEWS & WORLD REP., Jan. 23, 1995, at 55-56 (discussing "salami slicing," a pattern of electronic transfer-thefts from accounts in amounts so small that most account-holders would not recognize bank statement contained balance errors).

[4]So far, the Securities and Exchange Commission has sued Telephone Information Systems and affiliates on the grounds that their "cyberspace come-ons for an 'American Indian Lottery' were unregistered securities amounting to little more than high-tech pyramid schemes." Susan Antilla, *Market Place: Another First for Cyberspace! An S.E.C. Suit for Investor Fraud*, N.Y. TIMES, Mar. 16, 1995, at D10; *see also* Susan Antilla, *Has Cyberspace Got a Deal for You!*, N.Y. TIMES, Mar. 19, 1995, § 3 (Money & Business/Financial Desk), at 5 (describing electronic commerce offers, for example, for investment in a petroleum pipeline in Guatemala and in Huntway, a supplier for the West Coast of asphalt and producer of diesel fuel needed to run operations in "Yugoslavia").

[5]Benjamin Wittes, *The Dark Side of DIGITAL CASH*, LEGAL TIMES, Jan. 30, 1995, at 1. *See also Internet Aids Money Laundering Fraud Expert*, The Reuters Business Report, June 9, 1995, *available in* LEXIS, Nexis Library, Wires File (explaining that Internet and computer technology turned money laundering into a $300 billion worldwide activity).

[6]*See* William M. Bulkeley, *New On-Line Casinos May Thwart U.S. Laws*, WALL ST. J., May 10, 1995, at B1 (describing two companies that are setting up "on line" betting emporiums in Caribbean countries to skirt U.S. laws).

[7]*See* JOEL KURTZMAN, THE DEATH OF MONEY: HOW THE ELECTRONIC ECONOMY

tion, the new mechanisms operate just outside the scope of many national laws that apply to current "banking" transactions, including those that promote safety and soundness and deposit protection. As a result, we must consider the extent to which these changes will require the creation of new laws—both domestic and international.[8]

Legal standards for new electronic payments mechanisms should balance fair dealing and the need for certainty in the conduct of financial and related commercial transactions with the encouragement of innovation. Public acceptance of these payments mechanisms may depend on the chosen legal standards.[9]

Legal standards for these payments systems must focus on three areas of concern. First, to the extent possible, legal standards must avoid the costs that the current patchwork of national laws imposes on cross-border participants.[10] Next, the legal standards must create a level playing field between

---

HAS DESTABILIZED THE WORLD'S MARKETS AND CREATED FINANCIAL CHAOS 87-88, 92 (1993) (describing the inability of economists to measure the supply of money in the world and the creation of new financial instruments that has further reduced the ability of central banks to control the money supply). *See also* Wittes, *supra* note 5 (noting that the London Stock Exchange warned of growing danger for future regulation of financial markets from the Internet's worldwide web of computer networks).

[8]Research for this article identified the following nine areas for which these payment mechanisms will require new legal norms: (1) safety and soundness, (2) protection of participants whether they are commercial or consumer participants, (3) deterrence and prosecution of criminal conduct—particularly in terms of penetration and corruption of the payments mechanisms by criminal elements with a resulting loss of public acceptance of the affected payment systems, (4) monetary policy, (5) taxation (both tax avoidance and difficulties in fixing the situs of the taxable event), (6) antitrust, (7) privacy protection, (8) settlement rules and other rules pertaining to management of credit risks, and (9) pricing. Of course, more may arise—leaving much work for scholars and regulators alike.

[9]*See, e.g.*, Kawika Daguio, The History of Banks, the U.S. Government & Payment System Improvements: The past's implications for future payment systems including digital cash, the Columbia Graduate School of Business Conference on Electronic Commerce, 7 (April 20, 1995) (copy available on file with the author) ("Payment instruments should be convenient, cost-effective, safe and confidential to assure wide usage.... Cooperative efforts between banks as an industry and between banks and the government have made current payment instruments successful [sic] widely used, and can make future payment mechanisms similarly successful.").

[10]These involve bank regulation, telecommunications, data privacy and records retention, consumer-investor protection, and "bank secrecy" and anti-money laundering as they affect payments mechanisms. *See, e.g.*, Lisa A. Barbot, Comment, *Money Laundering: An International Challenge*, 3 TUL. J. INT'L. & COMP. L. 161, 181-82, nn. 96-102 (describing the different money laundering statutes in several countries).

heavily regulated banks and emerging, non-regulated non-bank competitors. Finally, these standards should facilitate cross-border transactions in recognition of the desirability of international legal standards for globally accessible payments mechanisms.

This article proposes baseline participant protections for these emerging payments mechanisms. It urges adoption of an international standard because of the numerous cross-border transactions that will occur and the nature of the new payments mechanisms. The principal objective of this Article is to stimulate discussion of norms for these payments systems in the legal, banking, and electronic commerce communities.

Part II of this article compares the fundamentals and the legal framework of these emerging payments mechanisms with those of current payment systems.[11] Part III examines various aspects of the emerging systems that require standards and proposes standards based on models from existing payments systems.[12] The proposed legal standards for new retail electronic payments systems are based on legal standards that regulate existing electronic payments mechanisms such as wholesale wire transfers[13] and electronic funds transfers.[14] The proposed standards also are based in part on standards governing paper-based payments systems, the law of sales, and

---

[11]*See infra* notes 20-127 and accompanying text.

[12]*See infra* notes 128-234 and accompanying text.

[13]Wholesale wire transfers in the United States are subject to Article 4A of the Uniform Commercial Code ("U.C.C."), which the majority of states adopted and which the Board of Governors of the Federal Reserve System adopted for its Fedwire transfer system. *See generally* U.C.C. § 4A (1995) (regulating funds transfers). In addition, in 1992, the United Nations completed work on the UNCITRAL Model Law on International Credit Transfers. G.A. Res. 47/34, U.N. GAOR, 47th Sess., Supp. No. 17, at 48-60, U.N. Doc. A/47/17) (1993) [hereinafter Credit Transfers Model Law]. For an excellent analysis comparing the model law with Article 4A of the U.C.C., see Carl Felsenfeld, *The Compatibility of the Uncitral Model Law on International Credit Transfers with Article 4A of the U.C.C.*, 60 FORDHAM L. REV. 53 (1992). As of early 1994, no nation had adopted the Model Law as local law. Permanent Editorial Board of the Uniform Commercial Code, *PEB Credit Transfers Commentary No. 13: The Place of Article 4A in a World of Electronic Funds Transfers* (Feb. 1994), *in* SELECTED COMMERCIAL STATUTES (West 1994) [hereinafter *P.E.B. No. 13*].

[14]Electronic funds transfers, the retail banking relatives of wholesale wire transfers, in the United States are subject to the federal Electronic Fund Transfer Act 15 § U.S.C. 1693-1693r (1994).

the purposes underlying the proposed New Uniform Payments Code as embodied in its 1982 "Introductory Memorandum by the Reporters."[15]

Part IV describes why we should undertake to provide standards for specific payments systems at this time.[16] Part V argues that we should begin with international standards for participant protections because of worldwide access to these payment mechanisms.[17]

Part VI briefly explains why a private or self-regulated set of rules would be preferable to individual government or international regulation. It suggests that the development of the standards be the task of a private international association or clearing house, such as SWIFT,[18] or a payment-system-specific sub-group of existing Internet working groups, such as The Internet Society.[19]

II. EXISTING AND NEW ELECTRONIC PAYMENTS SYSTEMS

A. Existing Electronic Payments Mechanisms

Electronic payments and electronic financial transactions are not new. The world's major funds transfer systems[20] move between $1 and $3 trillion

---

[15]Permanent Editorial Board for the Uniform Commercial Code, New Uniform Payments Code—P.E.B. Draft No. 2: Introductory Memorandum by the Reporters (Philadelphia, 1982) [hereinafter New Uniform Payments Code Report] (copy available on file with author).

[16]*See infra* notes 235-248 and accompanying text.

[17]*See infra* notes 249-258 and accompanying text.

[18]"SWIFT" is the acronym for the Society for Worldwide Interbank Financial Telecommunications, which is based in Belgium, and which began operations in 1977. As a third-party private network, SWIFT provides a communications network for a large number of international funds transfers. P. OPPENHEIM, INTERNATIONAL BANKING 95 (4th ed. 1983). For additional information on SWIFT's operations, see Hal S. Scott, *Corporate Wire Transfers and the Uniform New Payments Code*, 83 COLUM. L. REV. 1664, 1673-74 & n. 50-54 (1983).

[19]The Internet Society is one of several working groups supervising the development of the Internet in terms of commerce and technology. *See Internet Society to Hold Annual Conference in Prague*, PR Newswire, May 9, 1994, *available in* LEXIS, Nexis Library, CurNWS File (noting that annual conference is the "only global forum" dealing with worldwide Internet developments and technologies).

[20]"Funds transfers" refer primarily to credit transfers between banks or reflected on accounts held by banks and processed through long-established payments systems such as Fedwire, CHIPS, SWIFT, and CHAPS. Fedwire is the funds transfer system

daily.[21] The automated clearing houses ("ACH") in the United States originated more than 2.5 billion ACH items in 1994.[22] As of 1993, one expert identified twenty-one "major electronic networks around the world designed to move money."[23]

In addition, the world's major securities and commodities markets have round-the-clock, on- and off-exchange electronic trading through various Reuters' services such as Global Futures Exchange ("Globex"),[24]

---

operated by the 12 regional Federal Reserve Banks since 1918. U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, INFORMATION TECHNOLOGIES FOR CONTROL OF ELECTRONIC MONEY LAUNDERING 13, OTA-ITC-630 (1995) [hereinafter 1995 OTA PAPER].

CHIPS is the acronym for the Clearing House Interbank Payments System, which is a funds transfer system operated by the New York Clearing House Association since 1970. *Id.* at xii, 21-23. CHAPS is the acronym for the United Kingdom Clearing House Automated Payments System, which is a large-value transfer system operated by the clearing banks in the United Kingdom since 1984. BANK FOR INTERNATIONAL SETTLEMENTS, PAYMENTS SYSTEMS IN ELEVEN DEVELOPED COUNTRIES 57 (1985) [hereinafter DEVELOPED COUNTRIES' PAYMENTS SYSTEMS].

Some of the systems deliver messages that complete the transfer of funds to the beneficiary. Others, like SWIFT, only deliver instructions to pay the beneficiary and require a separate financial transaction (frequently on CHIPS) to complete the transfer of funds. Other funds transfer systems are in operation in a variety of developed countries. *Id.*

[21]In 1994, an average of more than 283,000 transfers were executed over Fedwire daily with an average daily dollar value of $812 billion. 1995 OTA PAPER, *supra* note 20, at 20. CHIPS' daily volume is approximately 200,000 transfers with a value of $1.2 trillion. *See* Steven Marjanovic, *N.Y. Clearing House Moving to Curb Risk in Settlements*, AM. BANKER, Aug. 3, 1995, at 17. CHIPS' largest volume of more than $1.95 trillion was reached on January 17, 1995. 1995 OTA PAPER, *supra* note 20, at 28-31.

[22]*The Future: Electronic Checks?*, CORP. EFT REP., Apr. 5, 1995, *available in* LEXIS, Nexis Library, NWLTRS File. Private ACH operators—those not using the clearing house services offered by the Federal Reserve Board—originated 580 million ACH items in 1994 or about 23% of the total. *Id.*

[23]KURTZMAN, *supra* note 7, at 183. Mr. Kurtzman noted that none of these payments systems were more secure with Fedwire, which suffered many breakdowns in the period from the middle 1980's through 1990. KURTZMAN, *supra* note 7, at 183.

[24]*See* KURTZMAN, *supra* note 7, at 28 (describing several round-the-clock trading systems). Globex is operated by the Chicago Mercantile Exchange and Reuters Holding PLC. Reuters also operates Dealing 2000 and Instinet.

and through services such as Aurora.[25] Banks, securities firms, and their customers also use telexes as means of giving payment or trading instructions.[26]

Existing wholesale and retail electronic payments mechanisms are within the provinces of exclusive bank clubs, or of other corporate financial service providers.[27] Existing electronic payments mechanisms share five key attributes. First, participants generally conduct these transactions using private, specially-designed, or limited-access networks.[28] Second, participants commonly base their transactions on pre-established accounts.[29] Third, the transacting parties are either well-known to each other, such as different subsidiaries of a large organization, or deal together only through well-known intermediaries, such as the world's largest commercial banks, long-established securities exchanges, or funds transfers systems.[30] Fourth, par-

---

[25]KURTZMAN, *supra* note 7, at 28. The Chicago Board of Trade operates Aurora. KURTZMAN, *supra* note 7, at 28.

[26]*See* Scott, *supra* note 18, at 1668–69, 1674 (describing wire transfers that may be completed, among other ways, by telex); DEVELOPED COUNTRIES' PAYMENTS SYSTEMS, *supra* note 20, at 19, 57 (noting the use of telexes for interbank credit transfers and other settlement obligations in Belgium and Japan, based on reports by central bankers at year's end, 1983). For additional information on telex methodology, see BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 1.1.3, (2d ed. 1991).

[27]Such as Fedwire, CHIPS, SWIFT, VISA International, MasterCard International, and American Express. In addition, auxiliary electronic payments systems, such as those provided by Western Union "Moneygrams" and First Data Corp. electronic transfers, offer corporations and consumers wholesale and retail payments services that operate in more than 100 different currencies and settle in roughly 25 currencies on a daily basis. Both Western Union and First Data are subsidiaries of American Express. Interview with Patrice Motz, Counsel, First Data Corporation, in New York, N.Y. (Sept. 27, 1995) [hereinafter Motz Interview].

[28]*See* 1992 OTA PAPER, *supra* note 2, at 7–14 (describing various types of networks available and explaining that in the 1980's and early 1990's major banks and other service providers shifted between private (internal only, shared, or value-added) and public networks to obtain telecommunications services necessary to support their electronic financial transactions).

[29]*See* Scott, *supra* note 18, at 1668, 1679–80 (describing wire transfers based on preestablished accounts). Moneygram and First Data transfers do not operate on the basis of accounts. Motz Interview, *supra* note 27.

[30]"Funds-transfer system" means a wire transfer network, automated clearing house, or other communication system of a clearing house or other association of banks through which a payment order by a bank may be transmitted to the bank to which the order is addressed. U.C.C. § 4A-105(a)(5).

ticipants follow specialized message formats[31] and individualized security precautions as need and technology permit.[32] Finally, participants conduct these transactions in accordance with payments systems rules that govern aspects of these transactions.[33]

Existing electronic payments systems enjoy a reputation for speed, security, and reliability.[34] This reputation contributed in part to the rapid

---

[31]SWIFT traditionally used the most comprehensive standard formats for its transfer messages, which aided processing and transmission of instructions to the banks required to transfer funds. *See* OPPENHEIM, *supra* note 18, at 95; 1992 OTA PAPER, *supra* note 2, at 10-11.

In 1992, CHIPS expanded its funds transfer communications "fields" to match SWIFT's and to carry more information about participants in specific funds transfers. American Bankers Association, Comment to the U.S. Department of the Treasury 5 (Jan. 15, 1991) (commenting on Proposed Amendments to the Bank Secrecy Act Regulations Relating to Recordkeeping for Funds Transfers by Banks and Transmittals of Funds by Other Financial Institutions, 55 Fed. Reg. 41,696 (1990) (proposing amendments to 31 C.F.R. § 103.33, codified at 31 C.F.R. 103.33(f)) (copy of comment available on file with author and available from Treasury). Fedwire currently requires minimal information—the amount transferred, the numbers of the accounts being debited and credited (which identifies the sending and receiving banks), the number of the beneficiary's account or other identifier, which identifies the beneficiary's bank. The Federal Reserve Board announced Fedwire's expansion in January, 1995. Federal Reserve Board, Notice of Service Enhancement, 60 Fed. Reg. 111 (1995) (to be implemented fully by year-end 1997).

[32]U.C.C. art. 4A pref. note. The prefatory note explains:

> To ensure that no unauthorized person is transmitting messages to the bank, the normal practice is to establish security procedures that usually involve the use of codes or identifying numbers or words. If the bank accepts a payment order that purports to be that of its customer after verifying its authenticity by complying with a security procedure agreed to by the customer and the bank, the customer is bound to pay the order even if it was not authorized. But there is an important limitation on this rule. The bank is entitled to payment in the case of an unauthorized order only if the courts find that the security procedure was a commercially reasonable method of providing security against unauthorized payment orders.

See U.C.C. § 4A-201 (1995) (security procedure); U.C.C. § 4A-202(c) (1995) (listing factors determining "commercial reasonableness of a security procedure").

[33]*See* U.C.C. art. 4A pref. note (1995) (stating that Fedwire transactions are governed by Federal Reserve Regulation J and CHIPS transfers are governed by CHIPS rules); Scott, *supra* note 18, at 1669-74 (describing the rules governing Fedwire, Bankwire, CHIPS, and SWIFT).

[34]C. Dianne Martin & Fred Weingarten, *The Less-Cash/Less-Check Society: Banking in the Information Age*, *in* ELINOR HARRIS SOLOMON, ELECTRONIC MONEY FLOWS: THE MOLDING OF A NEW FINANCIAL ORDER 187, 191-92 (1991) (citing Jerome Svigals, *EFT Technology Evolution: The Next 10 Years*, 1 EFT TODAY, Aug./Sept. 1988, at 9-11).

growth in volume that they have experienced in recent years.[35] Despite their good reputation, these systems have faced numerous challenges. First, for many years, wholesale funds transfer systems operated without benefit of domestic or international laws[36] until the adoption of Article 4A.[37] Second, originators of funds transfers and their banks either had limited contracts to govern these transfers, or no contract at all.[38] Third, funds transfer systems suffered break-downs and electrical failures that rendered them inoperable for hours at a time.[39] Fourth, they are vulnerable to hackers who pierce

---

[35]According to 1980 figures, electronic funds transfers accounted for the movement each year of $117 trillion. Scott, *supra* note 18, at 1664 & n.1. Fedwire's daily transfers of $1 to $2 trillion daily are more than twice the total value in 1983. *Compare* Laster & Wenninger, *supra* note 1, at 1, *with* Martin & Weingarten, *supra* note 34, at 191-192.

[36]*See* Scott, *supra* note 18, at 1678 & n.72 (noting that prior to adoption of U.C.C. Article 4A, disputes over bank wire transfers were "largely resolved by a gentleman's agreement" among members of a "small club" of domestic and international bankers involved in wire transactions that "broke down" after the number of banks offering wire transfers grew).

In 1991, the Federal Reserve Board amended the Regulation J provisions governing Fedwire to adopt Article 4A for all Fedwire transactions. 12 C.F.R. § 210 app. B (1993).

In the United States and Australia, funds transfers are subject to specialized regulations to preserve records of transfers as part of on-going efforts to deter or detect money laundering. 31 C.F.R. § 103 (1995) (enhanced recordkeeping requirements for funds transfers and funds transmittals promulgated by the Board of Governors of the Federal Reserve System and Department of the Treasury). Australia's AUSTRAC (the Australian Transaction Reports and Analysis Centre), the Australian Tax Office, and other Australian law enforcement agencies gather and analyze data on wire transfers for the purpose of detecting money laundering activities. 1995 OTA REPORT, *supra* note 20, at 48.

[37]Article 4A of the U.C.C. was the first regulation of "funds transfers" other than the rules of Fedwire, CHIPS, or SWIFT or the contracts of individual members of the funds transfer systems or between bank and customer wishing to originate funds transfers. *See* U.C.C. art. 4A pref. note (1995) (stating that no comprehensive body of law defining the rights and obligations that arise from wire transfers exists). Approved for state adoption in 1990, 49 states have adopted Article 4A.

[38]*See* U.C.C. art. 4A pref. note (explaining that resolution of many issues not covered by funds transfer system rules depend on parties' contracts or on analogy to law applicable to other payment systems). *Accord* Scott, *supra* note 18, at 1664 ("due to a lack of coverage and the limited use . . .").

[39]*See* KURTZMAN, *supra* note 7, at 182-83 (detailing multiple breakdowns in Fedwire from the middle 1980's through 1990 and noting the Federal Reserve System's intention to overcome these problems); Samantha Laurie, *Computers in Finance 8; The Burning Issue of Supervision—SWIFT: Faces Problems*, FIN. TIMES (Nov. 12, 1991), at art. VIII, survey (explaining that early reliability problems of SWIFT system interfered with European domestic clearing and end-of-day settlement).

their security systems.[40] Finally, in recent years money launderers and tax evaders have used these systems to obscure the beneficial ownership of funds by transferring funds through multiple accounts inside and outside the United States.[41]

B. Emerging Retail Electronic Payments Mechanisms

Since late 1994, banks and non-bank service providers have introduced a number of retail electronic payments options, including several forms of "digital cash." Among these new payment options are offerings by First Virtual Holdings, Inc. ("First Virtual"), and DigiCash BV ("DigiCash").

First Virtual offers to prospective purchasers from Internet vendors a trusted third-party, escrow-like security for their credit card numbers. The customer uses the First Virtual account number instead of her credit card account number in the on-line transaction and First Virtual charges the customer's credit card account for the amount authorized.[42] First Virtual's service thus protects the credit card number from misappropriation by computer hackers and from misuse by vendors.

DigiCash offers "electronic coins" to potential Internet purchasers; purchasers buy coins from DigiCash and pay for them by downloading value from their bank accounts to "electronic wallets" in their computers.[43]

---

[40]*See* John Markoff, *Software Security Flaw Puts Shoppers on Internet at Risk*, N.Y. TIMES, Sept. 19, 1995, at A1 (describing how two computer graduate students broke Netscape security code revealing easily broken security for credit card numbers); Jared Sandberg, *Netscape Software for Cruising Internet Is Found to Have Another Security Flaw*, WALL ST. J., Sept. 25, 1995, at B8 (detailing three security flaws in Netscape software and others in Unix software programs that also may affect confidential credit card or other personal data in Internet computers); William M. Carley & Timothy L. O'Brien, *Cyber Caper—How Citicorp System Was Raided and Funds Moved Around World*, WALL ST. J., Sept. 12, 1995, at 1 (discussing the international breach of Citicorp's electronic cash-management system).

[41]For example, the major funds transfers systems—and wholesale wire transfers themselves—had become the dominant means of laundering drug profits by the late 1980's. *American Bankers Association Money Laundering Task Force Report: Toward a New National Drug Policy—The Banking Industry Strategy*, 135 CONG. REC. S5555-56 (daily ed. May 18, 1989).

[42]Kim A. Strassel, *Dutch Software Concern Experiments with Electronic "Cash" in Cyberspace*, WALL ST. J., Apr. 17, 1995, at B6D.

[43]*Id.*

DigiCash's system also protects the purchaser's sensitive financial information from Internet thieves and offers more anonymity to purchasers concerned about data privacy.

In addition, on August 23, 1995, a consortium of banks and service providers including Citibank announced that they would begin to offer "electronic checking."[44] Proposed electronic checks would function mostly like paper-based checks but would be faster and more secure in terms of delivery.[45]

These new payment mechanisms arose because of commercial opportunities created by wide access to the Internet.[46] Commercial opportunities range from consumer and commercial purchases of goods, software, or information, to investments, foreign exchange, and cash movement.[47] The entrepreneurial nature of the Internet marketplace created the need for speedy, reliable, and secure[48] payment systems.

---

[44]Saul Hansell, *Checks Delivered Via E-Mail Are Planned*, N.Y. TIMES, Aug. 23, 1995, at D2; Steven Marjanovic & Jeffrey Kutler, *Chemical, Boston Bank to Show Internet "Check" in Two Months*, AM. BANKER, Aug. 25, 1995, at 1.

[45]*See* Marjanovic & Kutler, *supra* note 44, at 15 (discussing speed and security).

[46]Johanna Powell, *Hiding Technology's Power: It won't be as visible, but it will be far more sophisticated and helpful*, FIN. POST, Apr. 29, 1995, *available in* LEXIS, Nexis Library, CurNWS File (noting that an Internet study found that growth in terms of numbers of computers increased 132% over twelve months ending in April, 1995, while a U.S. study predicted that 8% of all transactions will be carried out over the Internet by the year 2000).

[47]The goods and services range from bulk coffee to marine equipment offered by some of the 60 on-line businesses active in Vermont-based Cybermalls, and other so-called "distance stuff," such as books, software, outdoor gear, packaged foods and collectibles, that people can buy without needing to touch them or try them on." Janice Castro, *Just Click to Buy—Madison Avenue Meets the On-Line World—and Neither Will Be the Same Again*," TIME, Spring 1995, at 74.

[48]*See* John Gapper, *The High Tech Art of Armchair Banking*, FIN. TIMES, June 10-11, 1995, at 7 (efforts to create secure method for credit card payments over Internet sponsored jointly by VISA and Microsoft; Barclays Bank (U.K.) launched electronic mall using encryption technology for credit card payments); Jared Sandberg, *Some Banks Bet the Internet Will Be the Medium*, WALL ST. J., June 8, 1995, at B1, B7 (quoting Susan Weeks, vice president of public affairs at Citibank, explaining that Citibank would not offer Internet banking "until we believe it's totally secure" and would continue plans to offer services through its private electronic banking network).

Concerns over security were raised anew with two disclosures in September, 1995. First, Citibank revealed that its cash management systems had been the victim of thefts of $400,000 and the attempts to steal more than $10 million by means of wire transfers initiated by a computer hacker located in the Russian Federation. John Mason, *Banks' Security Chains Rattled*, FIN. TIMES, Sept. 20, 1995, at 12; Carley & O'Brien, *supra* note

New retail electronic payment mechanisms currently exist in three forms, with at least two additional mechanisms scheduled for future operation. The three operational systems are: (1) payments services designed to protect credit card account numbers, such as the three-party escrows offered by First Virtual,[49] and "secure" credit card payments services offered by Wells Fargo Bank;[50] (2) "super-smart-cards" including pre-paid cards capable of storing sums for telephone calls or public transportation, as well as for other small and large-purchase transactions;[51] and (3) forms

---

40, at 1. *See also* John Markoff, *Security Flaw is Discovered in Software Used in Shopping*, N.Y. TIMES, Sept. 20, 1995, at A1 (revealing that Netscape security software contained a serious flaw allowing penetration of credit card numbers used in Internet commerce).

[49]Wendy Taylor, *They're Coming For Your Wallet! Electronic Currency; Reality Bytes*, PC-COMPUTING, Apr. 1995, at 150, *available in* LEXIS, Nexis Library, CurNWS File.

One of the key problems that appeared in early Internet purchase transactions was the risk of giving a credit card number and related validation information to a seller of goods or services over the Internet and of having the number misused by another Internet participant or even by the seller. *See Electronic Money; So Much for the Cashless Society*, THE ECON. Nov. 26, 1994, at 21 [hereinafter *Cashless Society*] (speculating on possible payment methods for goods over the Internet). Some buyers resist giving such potent information to an open forum such as the Internet. Other buyers dislike the prospect of making a separate telephone call to give the seller their credit card numbers; to the true Internet aficionado, the second communication severely hindered the speed and attractiveness of the Internet purchase, to say the very least. It also opened the door to unauthorized use of validation information for the credit card account by someone penetrating the system.

Some banking experts do not consider these secure credit card transactions as conceptually similar to "electronic money" because they operate like a regular credit card transaction in which the consumer card-holder "receives a bill for the purchases made on a regular credit card statement in the next billing cycle. . . ." Laster & Wenninger, *supra* note 1, at 6 n.1.

[50]*See* Markoff, *supra* note 40, at A1 (security flaws in software supporting payment systems such as this). For information on the original software for Netscape that was designed to ensure security for confidential data such as credit-card account numbers, *see* Netscape Products, Netscape Merchant System, *available at* http://homw.netscape.com/comprod/merchant.html (online order processing system processes credit card transactions, obtains authorizations, and issues electronic receipts) [hereinafter Netscape].

[51]Smart-card technology has existed for some time in western Europe and the United States where various entities have issued smart cards for repetitive, small-dollar purchases, such as transit fares and telephone calls. *See* Briggs Adams, *Card Offered for Fast Talkers and Frequent Fliers*, CHIC. LAWYER, Aug., 1995, at 68 (pre-paid phone cards circulating in Europe and Asia for a decade with total sales more than $4 billion).

Technology experts have predicted that smart cards would replace all small-dollar currency transactions—such as purchases of daily periodicals, soft drinks, and other vending machine items—as the cost of issuing and circulating currency rose. Laster & Wenninger, *supra* note 1, at 1.

of "private script," which include stored-value mechanisms such as those Mondex offers.[52] These stored-value cards are similar to telephone and transit value cards in circulation in the United States and Europe.

The two additional payment systems that have been announced, but are not yet operational, include (1) "electronic cash" systems that use prepaid bits of legal tender distributed by the national government or by banks and other financial service providers,[53] and (2) "electronic checks," which are electronic substitutes for paper-based orders to pay funds from an account.[54] This Article focuses primarily on announced private script and electronic check mechanisms.

1. Electronic Cash

Electronic or digital cash is a method of storing value electronically that is "transferable in real time between individuals and firms, or between

---

Smart cards are similar to "real money" in a number of respects that pertain to this discussion. First, they store value in a readily useable form. Second and third, respectively, but less happily, they are susceptible to the risk of loss or theft, and to the risk of counterfeiting. *See* Laster & Wenninger, *supra* note 1, at 2, 5, 13.

Super-smart cards are currently being offered by Mondex, a venture of National Westminster Bank (U.K.) in projects in Swindon, England, and in conjunction with Wells Fargo Bank in San Francisco, California. Tom Foremski, *Digital Cash in Your Chips—Issues such as money-laundering and evasion of taxes have yet to be dealt with satisfactorily/ Smart cards and electronic money, a UK trial attracted worldwide attention*, FIN. TIMES, Oct. 4, 1995, *available in* LEXIS, Nexis Library, CurNWS File (explaining details of Mondex systems). Rapidly developing technology will allow the same card to store value, contain access codes for a variety of accounts (bank accounts as well as traditional credit cards), and store biomedical and other data personal to the cardholder.

[52]*See* Foremski, *supra* note 51 (describing the Mondex card as one that stores digital money).

[53]Interview with Colin Crook, Senior Technical Officer, Citibank (CNN television broadcast Aug. 8, 1995), *available in* LEXIS, Nexis Library, Scripts File, Transcript No. 1151-5 [hereinafter Crook Interview] (predicting that it would take approximately ten years to get "real [electronic] money-bits of legal tender into circulation").

[54]Hansell, *supra* note 44, at D2; Marjanovic & Kutler, *supra* note 44. *See also*, U.C.C. §§ 3-103(a)(6); 3-104(a), (f) (1995) (defining "order," "negotiable instrument," and "check").

firms."[55] Electronic cash should offer three key benefits to participants: (1) finality of the payment transaction or "good funds,"[56] (2) some measure of data privacy for the participants,[57] and (3) anti-counterfeit measures.[58] Some of the systems currently operating, such as Mondex, also offer a fourth benefit in the form of peer-to-peer processing that eliminates the need for a financial intermediary to transfer the payment from buyer to seller.[59]

Electronic cash systems, such as that offered by DigiCash, require prospective purchasers to first establish an account.[60] The consumer next downloads value from a bank account to an "electronic wallet" in her computer in a process that is similar to retrieving cash from an automated teller machine ("ATM").[61] The consumer then may use digital coins to pay for pur-

---

[55]Daguio, *supra* note 9, at 9. *See also* First Bank of Internet, *Announcement: FBOI Opens, available at* fboi@netcom.com (detailing operation of Internet "cash" account offered by First Bank of Internet ("FBOI") and VISA International in conjunction with a FBOI-procured "VISA ATM Card" (automated teller machine card)). The Office of the Comptroller of the Currency and banking authorities in Illinois in May 1995, forced abandonment of this program on the ground that FBOI lacked requisite federal or state approval to accept "deposits." *See also* Amy Cortese & Kelly Holland, *What is the Color of Cybermoney*, BUS. WK., Feb. 27, 1995, at 80 (describing the problem of privacy when electronic payment systems are used).

[56]Dr. Daniel M. Schutzer, Vice President for Technology at Citibank, N.Y., Comments at the CITI Conference on Electronic Commerce, at Columbia University Graduate School of Business (Apr. 21, 1995) [hereinafter Schutzer Comments].

[57]Dr. David Chaum, Managing Director of DigiCash, Inc., Comments at the CITI Conference on Electronic Commerce, at Columbia University Graduate School of Business (Apr. 21, 1995) [hereinafter Chaum Comments].

[58]Schutzer Comments, *supra* note 56. DigiCash has features designed to ensure against the possibility of reuse of digital coins and against counterfeiting that entail marking each "coin" with a unique validating code and guarding that code from interception by the banks transferring the credit as well as from vendor and buyer. The DigiCash system also is designed to avoid interception of data and interruption by computer viruses. Chaum Comments, *supra* note 57.

[59]In the DigiCash system the seller may "deposit" the value in a traditional bank in order to use the value/funds for other extra-Internet purposes, or keep the value stored until required. Chaum Comments, *supra* note 57. The Mondex system allows holders to transfer value from card to card with the assistance of a hand-held computer developed by Oki of Japan and may redeposit stored value in the bank. Timothy Jones, Chief Executive Officer of Mondex International, Comments at the Cyberpayments Colloquium, U.S. Department of Treasury Financial Crimes Enforcement Network, at New York University School of Law (Sept. 27, 1995) [hereinafter Jones Comments].

[60]Cortese & Holland, *supra* note 55, at 80.

[61]The European Commission and a group of European banks are testing "electronic wallet" technology. Chaum Comments, *supra* note 57.

chases from Internet suppliers, who store them in the same form for their own later use or exchange them for credits in accounts at traditional banks.

Experts suggest that lay buyers' receptivity to digital cash may vary with the nature of the payment systems with which they are familiar. For example, experts anticipate that consumers in western Europe who are accustomed to smart cards and giro systems[62] will accept digital cash more readily than U.S. consumers.[63] One expert cautions that general acceptance will be slow because many consumers do not trust personal computers, let alone digital cash.[64]

For purposes of this article, it is necessary to "classify" or "describe"[65] "digital" cash, and to explain how characteristics of digital cash systems affect the types of risks inherent in electronic cash systems. These factors dictate the rules that these payments systems will require.

a. Legal Tender[66]

Experts have predicted that commercial markets will have to wait years for digitalized legal tender.[67] The prospect of digitalized legal tender raises larger questions of the convertibility of stored value to both "money"[68]

---

[62]For more information on giros, see JOHN F. DOLAN, UNIFORM COMMERCIAL CODE: TERMS AND TRANSACTIONS IN COMMERCIAL LAW 417-20 (1991).

[63]Richard Field, Comments at the CITI Conference on Electronic Commerce, Columbia University Graduate School of Business (Apr. 21, 1995) [hereinafter Field Comments]; John Wenninger, Comments at the CITI Conference on Electronic Commerce, Columbia University Graduate School of Business (Apr. 21, 1995) [hereinafter Wenninger Comments].

[64]Schutzer Comments, *supra* note 56.

[65]Taxonomists "classify" members of the same species and "describe" new species. Interview with Val K. Nolan, Professor (Emeritus), Indiana University School of Law (Nov. 3, 1995) (Professor Nolan is a noted ornithologist). For the apt use of the taxonomy construct, I am indebted to the Honorable Ronald K. Noble, former Under Secretary of the Treasury for Enforcement and Professor of Law at New York University School of Law, Remarks at the Cyberpayments Colloquium, U.S. Department of Treasury, Financial Crimes Enforcement Network, New York University School of Law, New York (Sept. 27, 1995).

[66]31 U.S.C. § 5103 (1994) (defining "legal tender").

[67]Crook Interview, *supra* note 53.

[68]E.g., U.C.C. § 1-201(24) (1995) ("[A] medium of exchange authorized or adopted by a domestic or foreign government . . . [including] a monetary unit of account established by an intergovernmental organization or by agreement between two or more nations.").

and other forms of value.[69] Digitalized legal tender would require issuance by the national government[70] and distribution through channels designed to minimize the opportunities for counterfeit tender to be in circulation.[71]

Digitalized legal tender, like paper currency and coins, would be susceptible to loss or theft. Guarding against loss or theft would require a system, such as registries of ownership of particular tender cards, similar to the current Federal Reserve Board policy of recording serial numbers of bills provided to the first bank to take possession.[72] Alternatively, the payment system could record the amount of tender stored in the card and the amount disbursed in any transaction each time the holder uses the card. Legislatures could adopt rules providing purchasers of lost or stolen tender cards or access devices with the equivalents of (1) "stop payment" authority,[73] and (2) the right to reimbursement for the balance of the card or device's value at the time of the stop order.[74] Among the disadvantages of ownership or use registries is their propensity to disturb the privacy offered by "cash" transactions.

---

[69]Commentators have predicted that:

> [m]uch will turn on the value which users of e-cash prove to attach to its convertibility into other forms of money. And here, one confronts questions that are related not merely to the Internet alone, nor indeed to electronic money alone, but are new-age cousins of the questions people asked when the first coins were struck, and when the first paper money was circulated, and when the first current accounts and credit cards were offered. The particular excitement of electronic money is that it poses the questions afresh in a pure, almost conceptual form: electronic money promises no intrinsic value, and barely even the trace of a physical existence. The Internet is about to push to the limit the question of what makes money worth what it is deemed to be worth.

Cashless Society, *supra* note 49, at 21, 22-23.

[70]*Cashless Society*, *supra* note 49, at 23.

[71]*Cf., e.g.*, *$100 Question: Will Ben's New Look Stop Counterfeits*, N.Y. TIMES, Sept. 28, 1995, at D19 (announcing redesign of U.S. paper currency to make it less susceptible to counterfeit).

[72]Interview with Robert Kaiman, Esq., Financial Crimes Enforcement Network, in Miami, Fla. (Oct. 12, 1995).

[73]U.C.C. § 4-403 (1995).

[74]Of course, questions of reliability of the reports of loss or theft would arise and would require rules to distribute losses should the person attempting to use the card or device have proof of lawful acquisition.

b. Private Script

Currently operating "electronic cash" systems involve two primary variations of private script. One expert refers to these variations as "net-around money" and "walk-around-money."[75] Internet commerce participants can use "net-around money" for on-line purchases, investments, and other value transfers but only in transactions with sellers who have suitable software. "Walk-around money" is more portable because it can be stored in smart cards or other small moveable access devices.

An example of "net-around money" are digital coins offered by DigiCash. DigiCash allows its customers to transform bank credits into digital coin credits.[76] Holders of digital coins may use them for Internet purchases, thus making them characteristic of "net-around money."

An example of "walk-around-money" are Mondex cards.[77] Holders of Mondex cards download value from bank accounts like DigiCash customers.[78] As with existing stored-value telephone and transit cards, Mondex card holders can use them in person where the counter-party has a card reader, which Mondex calls an "electronic purse."[79] Mondex card trials in the United Kingdom connect consumers with counter-parties such as grocers and newspaper stands. Consumers participating in the San Francisco trial can connect with the headquarters of Wells Fargo Bank and

---

[75]William Melton, founder of Verifone, Inc. and CEO of Cybercash, Remarks at the Cyberpayments Colloquium, U.S. Treasury, Financial Crimes Enforcement Network, New York University School of Law, Sept. 27, 1995.

[76]*See* Saul Hansell, *Today, Shoppers on Internet Get Access to Electronic Cash*, N.Y. TIMES, Oct. 23, 1995, at D4 (announcing joint venture between DigiCash BV and Mark Twain Bank of St. Louis, Missouri).

[77]Mondex is a proprietary card-based retail electronic payment system developed by a subsidiary of National Westminster Bank in the U.K., and also operated as a joint venture in the United States with Wells Fargo. *See* Foremski, *supra* note 51 (describing the Mondex smart card trial project).

[78]Foremski, *supra* note 51.

[79]Mondex's electronic purses may be stationary or portable. In the latter case, Mondex customers may use a hand-held "purse" that looks a great deal like a small cellular telephone. The purse allows Mondex customers to transfer value to another Mondex customer without the need of an intermediary, such as a bank or retailer. Jones Comments, *supra* note 59.

neighboring merchants such as Starbuck's Coffee.[80] Because of the wide availability of card readers in the trials and of Mondex's plans to expand participation,[81] Mondex's customers' opportunities to use the value stored appear to exceed uses for net-around money systems. In addition, although Mondex cards in many respects function like point-of-sale debit cards, holders also can transfer value to each other. As a result, Mondex cards function more like cash.[82]

Commentators express their reservations about private script digital cash systems. First, critics question the convertibility of digital cash to other payments systems and users.[83] To retrieve the value stored from the "electronic wallet" in which the digital coins sit, the customer must direct the coin issuer to make a reverse transfer from their wallet to a bank account. Successful completion of the reverse transfer, of course, will depend on the coin issuer's willingness and capacity to refund the value it previously received from the bank.

Second, commentators note that convertibility depends on the issuer's solvency at the time of the customer's request and the existence of contracts or legal standards supporting the reverse transfer.[84] Some commentators recall the era when individual U.S. banks offered bank notes[85] that were backed not by government securities, but by the issuer's promise to honor the notes' value.[86] Some commentators worry that electronic private script issuers may experience liquidity crises similar to those that affected 19th Century issuers of U.S. bank notes,[87] thus creating more generalized

---

[80]Foremski, *supra* note 51.

[81]*Id.*

[82]*Id.* Of course, cards like Mondex cards have the capacity to do more than store value. They are "access devices" for these payment systems and also at present have storage capacity suitable for personal information, including biomedical data, and other account access devices.

[83]Laster & Wenninger, *supra* note 1, at 4–5, 7–8, 13.

[84]*E.g.*, Laster & Wenninger, *supra* note 1, at 7–8.

[85]EDWARD L. SYMONS, JR., & JAMES J. WHITE, BANKING LAW 47 (3d ed. 1991); Laster & Wenninger, *supra* note 1, at 4.

[86]Laster & Wenninger, *supra* note 1, at 4.

[87]*E.g.*, Laster & Wenninger, *supra* note 1, at 8 (stating that consumers would be at greater risk in a nonbank network because a nonbank issuer of value would not be subject to the same regulation and supervision as a bank issuer).

uncertainty about private script that may result in a "drag on commerce."[88] Other commentators, although acknowledging the risks of private script, particularly of inadequate capital, are more optimistic and assume that the market will find appropriate solutions.[89]

The third common concern critics express regarding digital cash systems and other smart-card payment technologies (even those in which banks play a central role) is that these payment mechanisms do not constitute legal tender for all transactions.[90] In this respect, private script creates the possibility of competing currencies, both public and private. Some of these currencies will constitute legal tender for some purposes but not for others; some will involve only delivery of public benefits; some will be digitalized legal tender; and some will be strictly private script. Still others will be counterfeit. Commentators express concern that competing electronic currencies may devalue each other and hence pose a threat to monetary policy.[91]

2. Electronic "Checks"

Electronic checks[92] would have many of the properties of paper-based instruments as well as the convenience, speed, and security of electronic delivery. Electronic checks, like wholesale wire transfers, arguably offer more security than paper-based instruments because the account holder can control access to the account by highly specialized security devices and because

---

[88]Eugene Ludwig, Comptroller of the Currency, Remarks at the Cyperpayments Colloquium, U.S. Department of Treasury, Financial Crimes Enforcement Network, New York University School of Law (Sept. 27, 1995).

[89]Field Comments, *supra* note 63.

[90]Laster & Wenninger, *supra* note 1, at 4.

[91]*See* Laster & Wenninger, *supra* note 1, at 14–17 (analyzing monetary policy issues that might be raised by electronic money).

[92]For purposes of this Article, I have concentrated on rules appropriate for instruments drawn on banks. As this subset of the industry grows, it is likely that "electronic drafts" will appear. Rules for electronic drafts should have models similar to those I propose but also should accommodate existing differences in the legal status of drafts and checks.

digital signatures are harder to forge.[93] In addition, because the drawer delivers the payment instruction electronically to the payee, electronic checks are less likely to be stolen in transit or from the payee.

"Electronic checks" appear to be variants of regular checking or demand deposit account relationships as they exist in the United States Electronic checks, however, do not fit within the existing regulatory schemes available in the United States for paper-based checks, such as Articles 3 and 4 of the U.C.C., and Subpart A of Federal Reserve Board Regulation J.[94]

For example, although electronic checks do not qualify under the U.C.C. as "written instructions to pay money,"[95] they may be considered "signed"[96] by the "drawer" sufficiently for U.C.C.'s validation purposes. Of course, with paper-based checks and drafts, both the writing and the signature are validation devices. Electronic checks apparently will have only one of the two standard forms of validation.

On the positive side, electronic checks and drafts are similar to paper-based instruments, because they are account-based.[97] In addition, electronic

---

[93]DigiCash BV, "Welcome to the DigiCash Webserver," at "about ecash" and Figure 11, *reprinted in* UNITED STATES DEPARTMENT OF THE TREASURY, FINANCIAL CRIMES ENFORCEMENT NETWORK, EXPLORING THE WORLD OF CYBERPAYMENTS, AN INTRODUCTORY SURVEY at Appendix I (Examples of Cyberpayment Systems as described on the Worldwide Web) (Sept. 27, 1995) [hereinafter "FinCen Report"] (describing techniques making digital signature in coin form difficult to counterfeit or forge) (copy available from the author). *Cf.* Laster & Wenninger, *supra* note 1, at 13 (arguing that "it remains an open question whether it will be easier to protect monetary value in a paper or in an electronic environment").

[94]Collection of Checks and Other Items By Federal Reserve Banks, 12 C.F.R. § 210 subpt. A (1995).

[95]U.C.C. § 3-103(a)(6) (1995) (defining "order," which encompasses both "checks" drawn on "banks" and "drafts" drawn on drawees other than banks). Writings also must be signed "by the person giving the instruction." U.C.C. § 3-103(a)(6) (1995).

[96]U.C.C. § 1-201(39) (1995) (defining "signed"). Thus, if the validation device (digital signature/algorithmic string) is treated as a "symbol executed or adopted . . . with present intention to authenticate a writing," the device might qualify as a "signature" for this purpose. U.C.C. § 1-201(39) (1995).

[97]Account-based electronic payments mechanisms, including wholesale wire transfers, offer the collateral benefit of leaving a trail with which to monitor criminally suspicious transactions—whether based on activity observable by humans or on artificial intelligence programs being deployed by major financial institutions for detection of credit risks and of money laundering or fraud. *See* 1995 OTA PAPER, *supra* note 20, at 54–55 (Table 4-2: "Current Monitoring and Compliance Systems"), 67 (Table 4-3: "Electronic Fraud Detection at the Travelers Insurance Company").

payments mechanisms follow current initiatives to reduce the cost of collecting payments, such as electronic presentment[98] and check truncation.[99] They also meet the longstanding policy, established in part by the Expedited Funds Availability Act of 1987, of curtailing certain credit risks by hastening the speed of collection by limiting opportunities for "float."[100]

On the negative side, because the communication medium for the payment increases risks of misdescription of the beneficiary of the payment or misdirection of the payment, it may be more difficult to establish either

---

[98]Electronic presentment together with check truncation are methods of reducing the costs of check collection. *See* Phil Brit, *Electronic Checks Ready for Takeoff: Electronic Check Presentment*, 4 AM. COMMUNITY BANKER, Aug. 1995, at 19 (explaining that institutions reluctant to start electronic presentment choose imaging and check truncation); Data Exchange, ABA BANKING J., Mar. 1995, at 74 (describing how Federal Reserve Bank of Minneapolis to offer image processing and advanced check truncation services). Revised Article 4 expressly provides for electronic presentment. U.C.C. § 4-110 (1995).

[99]Check truncation eliminates:

> the physical handling of paper checks at some point of the check collection process. The data necessary to process the check is obtained through MICR [Micro Incoded Character Recognition] technology.... Currently, banks seldom use check truncation in consumer transactions; however, credit unions normally truncate their consumer's share drafts which are check-like equivalents.... The actual paper drafts have been copied then destroyed.... Active participation by banks in the check truncation process would reduce the processing costs associated with check collection. Because check truncation expedites the collection process, the time period between the issuance of a check and the final payment would be shortened, decreasing the "float," and shortening the holding period necessary for banks to determine whether a check ultimately will be honored.

RICHARD E. SPEIDEL, ET AL., PAYMENT SYSTEMS 264-65 (5th ed. 1993).

One of the features of the 1990 revision to Article 4 of the U.C.C. was the addition of specific provisions applicable to agreements between collecting banks and payor banks pertaining to truncation. U.C.C. § 4-209(b) (1990). Another facilitates bank-customer agreements to truncate processed and paid checks at the payor bank. U.C.C. § 4-406(a) (1990). Original Article 4 also allowed for the possibility of truncation. U.C.C. § 4-406(1) (1989).

[100]12 U.S.C. §§ 4001-4010 (1994), *as implemented by* Federal Reserve Board Regulation CC, 12 C.F.R. § 229 (as amended) (1995). *See* Knudson et al., *supra* note 1, at 269-70. The term "float" refers to the time value of deposits between the time the depositor delivers an instruction or order to pay and the time the payee-beneficiary actually collects the funds represented by the institution or order to pay. Professors Speidel, Summers, and White define "float" as "[arising] when the payee takes [a] check in at least provisional settlement for a debt at a time when the bank on which it is drawn has not debited the account. Thus, in effect, the depositor doubles her money. The bank treats her as though she has money in the bank and the merchant treats her as though she has paid." SPEIDEL ET. AL., *supra* note 99, at 256. The Federal Reserve Board has concentrated on reducing float as a means of controlling payment

ownership of the check or identify the agency to enforce it should ownership or entitlement disputes arise.[101] As a result, drawers may face increased risks of "double payment" of electronic checks, i.e., having two parties demand payment of the same check.[102]

A real question exists about the taxonomy of electronic checks. To the extent that banks continue to serve as the drawees of these "checks," the law could classify them as traditional checks, differing only in terms of delivery methodology to the payee and the collection process. If this were the case, the rules in Articles 3 and 4 of the U.C.C. or the 1989 UNCITRAL Convention on International Bills of Exchange and Promissory Notes could serve as models for participant protections that would apply, respectively, directly or by analogy to electronic checks. Alternatively, the law might describe electronic checks as a new species of payment system more closely related to other existing electronic payment mechanisms. For example, they could constitute sub-groups of funds transfers that are governed by funds

---

system risk since at least 1983. SPEIDEL ET AL., *supra* note 99, at 253. *See, e.g.*, 50 Fed. Reg. 47,752 (1985) (Federal Reserve Board proposed several measures to reduce Federal Reserve float); 48 Fed. Reg. 20,802 (1983) (approving proposals to reduce and price Federal Reserve Check float).

[101]Some commentators believe that both tasks will be easier, rather than harder, because of the greater degree of security that will emerge under cyberpayments systems. *See* Chaum Comments, *supra* note 57; Jones Comments, *supra* note 59. Articles 3 and 4A provide models for rules on establishment of entitlement to pay and on liability of the account holder in the event of misdescription of the beneficiary or misdirection of the payment. *E.g.*, U.C.C. §§ 3-301 (Person Entitled to Enforce Instrument), 3-309 (Enforcement of Lost, Destroyed, or Stolen Instrument), 3-312 (Lost, Destroyed, or Stolen Cashier's Check, Teller's Check, or Certified Check), 4A-207 (Misdescription of Beneficiary), 4A-208 (Misdescription of Intermediary Bank or Beneficiary's Bank) (1995).

[102]The risk of double payment is great in any case in which paper-based checks are stolen from or lost by the rightful owner. As a result, the law of negotiable instruments has emphasized possession of the instrument as a key element of proof of entitlement to pay. U.C.C. §§ 1-201(20), 3-301 (1995). Of course, instruments are lost and stolen and, to reduce the risk of double payment, parties to instruments need rules to help decide who is entitled to payment. U.C.C. Article 3 provides two sets of rules for proof of ownership for lost or stolen instruments, depending on the precise nature of the instrument in issue (note, check, cashier's check, teller's check, certified check). U.C.C. §§ 3-309, 3-312(a)(1) (1995). It also provides that discharge of the obligation to pay results only when the instrument is paid to the owner or the owner's agent. U.C.C. § 3-602 (1995).

transfer system rules[103] and Article 4A of the U.C.C. Article 4A applies exclusively to "push" transactions or credit transfers.[104]

Finally, the law could classify electronic checks. Electronic checks and security devices (personal identification numbers or digital signatures) required to activate them might be classified as "access devices" for purposes of the Electronic Fund Transfer Act ("EFTA").[105] Because the EFTA defines "electronic fund transfer" to encompass both debit (pull) and credit (push) transfers that affect an account, the EFTA is likely to cover electronic checks.[106]

---

[103]These of course include Subpart B of Federal Reserve Board Regulation J for the Fedwire system. 12 C.F.R. § 210 (1995).

[104]U.C.C. art. 4A pref. note (1995); U.C.C. § 4A-103(a)(1) (1995) (defining "payment order"). In "push" transactions, the originator sends bank credits towards the payee/beneficiary without receipt by the payee of the payment instruction or other action required of the payee thus pushing the payment away from its depositary account. However, checks traditionally are considered as "pull" transactions. In "pull" transactions, the payee receives the instruction needed to obtain payment and initiates collection, pulling the payment into its depositary account. Scott, *supra* note 18, at 1667.

The other type of credit transfer in the U.S. is the "automated clearing house" ("ACH") transfer. ACH rules apply to instructions given in batches to pay many payees. EDWARD L. RUBIN & ROBERT COOTER, THE PAYMENT SYSTEM 837-38, 867-69 (2d ed. 1994). This "batch" characteristic of ACH payments makes ACH an unlikely model for rules for electronic checks.

[105]15 U.S.C. §§ 1693-1693r (1994), *implemented by* 12 C.F.R. § 205.2(a)(1) (1985) (defining "access device" as "a card, code, or other means of access to a customer's account, or any combination thereof, that may be used by the consumer for the purpose of initiating electronic fund transfers"); 12 C.F.R. § 205.2(g) (1995) (defining electronic fund transfer). *See* Laster & Wenninger, *supra* note 1, at 9-10 (discussing how Regulation E would apply to electronic money issued by banks on prepaid credit cards, like ATM and debit cards, the prepaid card would serve as an account access device when down-loading value from a checking account onto the card).

[106]*E.g.*, Hansell, *supra* note 44 (describing how a group of banks and technology companies that will design a system to create "electronic checks" to be used to make payments over the Internet and other electronic mail systems); Marjanovic & Kutler, *supra* note 44 (stating that electronic check transactions will more often than not fall under Regulation E, the consumer protection rules for electronic funds transfers). Indeed, methodologies such as First Virtual's appear to involve "access devices" and to come under the umbrella of the Act because the alias allows the customer and vendor to access the account that the credit card represents. *See supra* notes 1-19 and accompanying text.

There are several disadvantages of subjecting electronic checks to the EFTA, including: (1) the Act's liability limits,[107] (2) its "error resolution" protocol,[108] and (3) its scope as a "consumer" protection scheme.[109] Because of the EFTA's limited applicability, drawees and payees would face the prospect of distinguishing between *personal* electronic checks that would be subject to the Act, and *corporate* electronic checks that would not be. Thus, drawees and payees might have to process the different groups accordingly. Application of the EFTA would result in markedly different rules governing otherwise identical payment mechanisms, in addition to higher processing costs.

A major problem with electronic checks would arise if the drawer were in one country and the payee in another. In these cases, if electronic checks were treated as "checks," the UN Convention would not apply,[110] and ordinary choice of law protocols would govern. Cross-border payment by checks under current law would increase both costs and risks of collection.

Finally, electronic checks present different demands than paper-based instruments including validating the identity of the drawer or issuer of the payment instruction, identifying the person entitled to enforce such instruction, and determining rules governing the absence of authority to issue the instruction.[111] Electronic checks also may complicate detection of alterations.

In the United States, three sets of rules are available as models to resolve different demands inherent in electronic checks. First, Articles 3 and 4 of the

---

[107]15 U.S.C. § 1693g (1994) (ranging from $0 to $500 or more depending on the circumstances surrounding the loss and the point at which the consumer notifies the financial institution that issued the access device).

[108]15 U.S.C. § 1693f (1994); 12 C.F.R. § 205.11 (1995).

[109]15 U.S.C. § 1693a(2) (1994); 12 C.F.R. § 205.2(b) (1995) (defining "account" to include only those maintained for "personal, family, or household purposes.").

[110]Felsenfeld, *supra* note 13, at 66–67 (describing problems when similar wire transfers are governed by the U.C.C. if wholly domestic transfers and by the Credit Transfers Model Law if cross-border transfer).

[111]*See* U.C.C. § 3-401(a) (1995) (stating that persons not liable on instrument unless signed by person or person's agent and signature is binding on represented person under § 3-402); U.C.C. § 3-403 (1995) (stating an unauthorized signature is ineffective except in favor of a person who in good faith pays the instrument or takes it for value).

U.C.C. deal with all three issues through a variety of rules,[112] including the warranties arising by transfer or presentment of the payment instrument.[113] Second, Article 4A deals with the same type of issues as recast in the context of wholesale wire transfers.[114] Article 4A also contains rules governing responsibility for erroneous payment orders[115] and erroneous executions of otherwise valid payment orders[116] that may assist in designing rules appropriate for electronic checks. Finally, the EFTA and Federal Reserve Board Regulation E provide validation rules and error resolution procedures for consumer electronic fund transfers.[117]

C. Distinctions Between Existing and Emerging Payments Mechanisms

In contrast to existing payments systems, new retail electronic payments systems lack uniform terminology and a reliable taxonomy.[118] These features limit the ability to frame legal issues and rules for these payments systems. Additionally, four attributes distinguish the new retail electronic payments systems from their predecessors. First, emerging electronic payments systems are more likely to operate over public networks, such as the Internet, than

---

[112]*E.g.*, U.C.C. § 3-103(a)(6) (1995) (defining "order" as a written instruction to pay money signed by the person giving instruction); U.C.C. § 3-301 (1995) (person entitled to enforce instrument); U.C.C. § 3-302(a)(1) (1995) (holder in due course); U.C.C. § 3-308(a) (1995) (proof of signatures and status as holder in due course); U.C.C. § 3-406 (1995) (negligence contributing to forged signature or alteration of instrument); U.C.C. § 4-401(a) (1995) (stating that bank may charge against customer's account an item properly payable from that account even though charge creates an overdraft).

[113]*E.g.*, U.C.C. § 3-416 (1995) (transfer warranties); U.C.C. § 4-208 (1995) (same).

[114]*E.g.*, U.C.C. §§ 4A-201 to 4A-204 (1995) (dealing with Security Procedure; Authorized and Verified Payment Orders; Unenforceability of Certain Verified Payment Orders; and Refund of Payment and Duty of Customer to Report With Respect to Unauthorized Payment Order).

[115]U.C.C. § 4A-205 (1995) (Erroneous Payment Orders).

[116]U.C.C. § 4A-303 (1995) (Erroneous Execution of Payment Order).

[117]15 U.S.C. § 1693a(1) (1994) (means of access); 15 U.S.C. § 1693a(11) (1994) (unauthorized electronic funds transfer); 15 U.S.C. § 1693f (1994) (error resolution).

[118]FinCEN, Exploring the World of Cyberpayments, An Introductory Survey (Sept. 27, 1995) (copy on file with author).

over dedicated private networks.[119] The public nature of the communications and payment media exposes them to increased risks of unauthorized transactions and alterations, insider abuses, and even outsider penetration[120] than are present in the private networks.[121]

Second, transactions using new retail electronic payments mechanisms may not be associated with an existing "account," and therefore, may lack protections afforded to participants through reserve or margin requirements that aid public acceptance of payment or trading systems.[122]

Third, some participants in these new payments systems will be less sophisticated than the corporate and banking participants in existing funds transfer systems,[123] and also may be more protective of their privacy than

---

[119]Private networks were the communications vehicle for existing wholesale wire transfer systems and automated clearing house systems, internal banking and securities communications systems, commodities trading networks, and other electronic financial service systems until very recently. 1992 OTA PAPER, *supra* note 2, at 15-16. One exception was the telex, which travelled over public communications networks, but for security reasons travelled in highly encrypted form. Scott, *supra* note 18, at 1674.

[120]Holland, *supra* note 3, at 96.

[121]Unauthorized transactions do occur in the major funds transfer systems. Carley & O'Brien, *supra* note 40, at A1 (detailing numerous penetrations of Citicorp's internal funds transfer computer systems and unauthorized transfers of more than $10 million). *See* U.C.C. § 4A-203, Official Comment 2 (1995) (listing examples of fraudulent wire transfers where the customer is not liable to pay the order and the receiving bank takes the loss); U.C.C. art. 4A pref. note (discussing requirement that bank use commercially reasonable security procedures to ensure that customer pays for unauthorized payment order in a wire transfer).

[122]*See* KURTZMAN, *supra* note 7, at 153 (margin requirements differ among competing markets, viz., five to ten percent for commodities deals), 159 (five percent margin for Treasury bond futures); Laster & Wenninger, *supra* note 1, at 3-9 (analysis of asset and liability character of electronic money). Bank regulators and funds transfer systems have been able to increase the levels of protection against credit risks for existing electronic payments systems through reserve requirements or other types of collateral. 1992 OTA PAPER, *supra* note 2, at 33-35. For more (but somewhat dated) information on payment risk, see E.J. Stevens, Federal Reserve Bank of Cleveland, *Payment System Risk Issues*, ECON. COMMENTARY, June 15, 1989 (making assessment that predates 1990 changes to CHIPS to reduce payment system risk); DEVELOPED COUNTRIES' PAYMENT SYSTEMS, *supra* note 20, at 3.

[123]*See* U.C.C. art. 4A pref. note (discussing characteristic funds transfers as typically "multimillion dollar transactions" between "especially sophisticated business or financial organizations").

existing payments systems participants.[124] Indeed, some participants in the new systems may be interested in these systems precisely because they offer more anonymity than traditional payments systems.[125] Finally, emerging retail electronic payments systems are likely to operate with little or no government regulation to promote safety and soundness[126] or consumer protection.[127]

III. WHAT ISSUES REQUIRE STANDARDS AT THIS TIME?

As previously noted, acceptance by the general public of new retail electronic payments systems depends on their speed, reliability, and security. Speed, of course, is not the primary concern of this Article.[128] Reliability and security are matters of concern in all retail banking and financial service transactions and are matters of special concern whenever the payments system depends on electronic media. Given the pace with which these payments systems are evolving, we need to adopt baseline legal standards that provide appropriate protection and are sufficiently flexible to allow for innovation.

---

[124]This factor together with desire for anonymity in transactions will complicate scrutiny of transactions for purposes such as detecting money laundering. Vic Sussman, *Policing Cyberspace*, U.S. NEWS & WORLD REP., Jan. 23, 1995, at 54.

[125]*Id. Accord*, Cortese & Holland, *supra* note 55, at 36 (once encrypted money leaves bank account, electronic cash cannot be traced to customer).

[126]*E.g.*, Laster & Wenninger, *supra* note 1, at 8. Other "electronic money" service-providers will attract the attention of regulators if they stray into regulated activities such as deposit-taking. For example, in May 1995, the U.S. Office of the Comptroller of the Currency issued an advisory warning First Bank of the Internet in Des Plaines, Illinois, that it lacked both a bank charter and federal deposit insurance necessary to accept "deposits" as it had advertised it would over the Internet. Cortese & Holland, *supra* note 55, at 66.

[127]Laster & Wenninger, *supra* note 1, at 4 (bank-issued prepaid smart cards not tender). Some of the smart cards will be covered by the EFTA. Others may not because they will not operate on the basis of established "accounts" as that term is defined in Section 903 of EFTA because they are not means of accessing "accounts" at "financial institutions." Congress may exempt stored-value smart cards from EFTA coverage. Where the EFTA does not apply, users will lack basic consumer protections it affords viz., documentation of transfers, error resolution, and liability for unauthorized transfers.

To the extent that they are not operated by banks, Article 4A of the U.C.C. will not govern these transactions and neither will the Model Law on International Credit Transfers.

[128]*See supra* notes 34–41 and accompanying text.

Part III of this Article focuses on subjects for which there is the greatest need to have baseline protection and for which competing regulatory models for different payments mechanisms—electronic fund transfers,[129] wholesale wire transfers, and checks—offer different answers to particular problems. Part III of this Article identifies important distinctions between electronic cash and electronic checks and drafts.[130]

A. Reliability Rules

Counter-parties in electronic transactions need assurance that the transactions in which they participate are reliable. The buyer-sender wants protection against the dissembling or non-performing seller-beneficiary. The seller wants assurance that the buyer cannot avoid payment after accepting the benefit of the bargain. The absence of face-to-face dealings in electronic transactions undoubtedly magnifies the need for these assurances.

---

[129]The EFTA does not apply perfectly to all aspects of electronic cash and electronic check transactions. For example, the Act applies only to consumer transactions. In addition, the Act's definition of "electronic fund transfer" includes "any transfer of funds . . . initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape" but restricts the term to those transfers that "order, instruct, or authorize a *financial institution* to debit or credit an account." 15 U.S.C. § 1693(a)(6) (1994) (emphasis added). Thus, to the extent that new retail payments systems involve service providers that are not "financial institutions" within the Act's definition, the Act will not apply. 15 U.S.C. § 1693(a)(8) (1994). DigiCash transfers, accordingly, will not be covered at the stage when the customer effects payment to the vendor. *Accord*, Laster & Wenninger, *supra* note 1, at 9-10. At the time of this writing, Congress is considering an exemption from the EFTA for certain stored-value cards (primarily because it would be too burdensome to require vending machines for beverages and newspapers to dispense a receipt for each transaction although the EFTA requires that the consumer receive a receipt). H.R. 2158, 104th Cong., 1st Sess. (1995); S. 1270, 104th Cong., 1st Sess. (1995).

In addition to federal regulations on electronic fund transfers, two states—Michigan and Wisconsin—have enacted laws to protect the rights of holders of electronic fund transfer access devices. WIS. STAT. § 943.41 (1994); MICH. STAT. ANN. § 28.354(13) (1993) (Callaghan 1993).

[130]In conjunction with this portion of the Article, the term "electronic fund transfer" refers to the consumer payment system currently governed by the EFTA; the term "wholesale wire transfer" refers to those credit transfers governed by Article 4A of the U.C.C. (where enacted) and by Federal Reserve Board Regulation J if conducted by Fedwire or by rules of the funds transfer systems such as SWIFT and CHIPS. The term "checks" refers to paper-based orders to pay such as those governed in the United States by Articles 3 and 4 of the U.C.C. and by Federal Reserve Board Regulations J and CC. 12 C.F.R. § 210 (1990); 12 C.F.R. § 229 (1992).

Reliability rules common to both electronic cash and electronic drafts include rules for (1) verification of the buyer-sender's identity or authority to use the access device; (2) erroneous execution (whether wrong beneficiary, wrong amount, or duplicate executions); (3) system failure; (4) stop payment or reversibility of payment; (5) date when payment occurs; and (6) discharge by payment of the underlying obligation.

1. Electronic Cash

Electronic cash transactions have elements of both existing retail and wholesale wire transfers in terms of the types of reliability problems that may arise. They are similar to retail electronic fund transfers in that they require an "access device"[131] and their users will include persons who have "personal, family, or household purposes" for using the payment mechanisms.[132] Whether or not Congress exempts "stored-value" cards from the EFTA, solutions to the issues associated with these cards must be derived from sources other than the EFTA, particularly where they arise across national borders.[133]

a. Verifiability of the Transaction and Related Topics

Counter-parties in electronic cash transactions have a variety of concerns that fall under the general category of transaction verifiability. These include security procedures to ensure that the sender is authorized to initiate the transaction, means of identifying and reporting errors, and means of cancelling or amending the transaction.

(i) Security Procedures and Means of Initiating Transactions

The EFTA and Article 4A address security procedures and means of controlling initiation of transactions rather differently. The EFTA relies on the duality of the "access device"[134] and a "personal identification

---

[131]12 C.F.R. § 205.2(a)(1) (1995).

[132]15 U.S.C. § 1693a(2) (1994); 12 C.F.R. § 205.2(b) (1995).

[133]An ABA working group on international electronic fund transfers, chaired by Roland Brandel, is studying this issue.

[134]12 C.F.R. § 205 (1995). Access devices commonly are moveable plastic cards with electronic stripes that consumers use together with a personal identification number to gain access to their accounts. *See* SPEIDEL ET AL., *supra* note 99, at 416.

number'' (''PIN'') as the exclusive means by which the account-holder may enter the system. Transfers in which both the correct access device and personal identification number are present generally demonstrate authority from the account-holder to initiate the transfer.[135]

Article 4A handles verifiability by various approaches depending on the means by which the sender ''sends'' each individual ''payment order.''[136] Generally, the recipient (receiving bank) tests the payment order to prove that the sender is who it purports to be. Article 4A requires senders and receiving banks to contract regarding the type of test the parties will use.[137] Article 4A uses the term ''security procedures'' for these tests.[138] Article 4A requires that the security procedure be ''commercially reasonable'' in terms of the requirements and situation of the sender.[139]

Electronic payments systems and financial electronic data interchange systems will utilize security procedures such as ''digital signatures.''[140] Electronic cash systems, such as that offered by DigiCash, appear to follow the security protocol required by Article 4A. DigiCash also encrypts the value

---

[135]For a matter in which this convergence of access device and PIN did not demonstrate authority to conduct the transfer, see Joanne Johnson, *Suspect in ATM Scam Pleads Guilty to Conspiracy Charges: ATM Scam Suspect Enters Guilty Plea*, THE HARTFORD COURANT, Sept. 25, 1993, at B1 (explaining how thieves installed a fake ATM in a shopping mall and recorded customer code information then using counterfeit cards and stolen personal identification numbers to withdraw cash from ATM's in New York City).

[136]Article 4A allows fund transfer participants to agree on specialized procedures for authenticating paper-based payment orders, those delivered by telephone, and those delivered by dedicated computer lines.

[137]U.C.C. § 4A-202 (1995).

[138]Article 4A defines the term ''security procedure'' as:

> a procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices. Comparison of a signature on a payment order or communication with the authorized specimen signature of the customer is not by itself a security procedure.

U.C.C. § 4A-201 (1995).

[139]U.C.C. § 4A-202(b)(i) (1995).

[140]Digital signatures are specially designed and theoretically unique algorithmic strings.

stored in the customer's electronic wallet to protect the customer's privacy and to assure that the vendor receives "good funds."[141]

(ii) Identifying and Reporting Errors

In addition to the heightened problems associated with verifying customers' instructions and ensuring their authority to give such instructions, electronic payments systems suffer risks of erroneous execution.[142] In electronic cash transactions, erroneous execution risks apply both to the transfer in which the customer downloads value to the customer's computer and to the transfer in which the customer transfers this value to the seller to make a purchase. In both cases, the recipient of the instruction to move value may have no reason to know that an error exists.

There are three ways, however, that the sender should recognize errors. First, the sender's "electronic wallet" (where the system stores value) may not contain the value downloaded. Second, it may contain too much. Finally, the account from which the sender downloaded value may still contain all that was present before the attempt to download. For these types of errors, rules for electronic cash transactions can follow Article 4A, which places the burden on the sender to detect and report errors.[143] In addition, Article 4A places the burdens on the sender to prove that (1) it followed the requisite security procedure and (2) the error would not have occurred unless the intermediary or beneficiary in the payment system had followed the security procedure.[144] Depending on the nature of the error,[145] the sender

---

[141]*See* PHYLLIS K. SOKOL, EDI: THE COMPETITIVE EDGE 57–58, 60–61 (1989) (explaining the coded validation devices in electronic data interchange transactions).

[142]"Erroneous execution" includes three types of errors: payments made to the wrong party, payments made in the wrong amount, or payments made in duplicate.

[143]U.C.C. § 4A-204 (1995) (Refund of Payment and Duty of Customer to Report with Respect to Unauthorized Payment Order) (creating duty of sender to report unauthorized payment order); § 4A-304 (1995) (Duty of Sender to Report Erroneously Executed Payment Order) (creating duty to report erroneously executed payment orders). Under these provisions, the sender has a duty to report within a reasonable time "not exceeding 90 days after the notification [revealing the error] from the bank . . . by the sender." The sender's time for reporting effectively is shortened by Federal Reserve Board Regulation J to "30 calendar days" after the sender receives notice that the payment order was accepted or executed or that the sender's account was debited for the transfer. 12 C.F.R. § 210.28 (1992) (Agreement of Sender).

[144]U.C.C. § 4A-205(a)(1) (1995).

[145]The three forms of error are execution to the wrong beneficiary, duplicate execution, and execution in an amount greater than intended by the sender. U.C.C. §§ 4A-207, 4A-303(a) (1995). Article 4A has additional rules governing misdescription

of value either has no obligation to pay or has an obligation limited to the amount the sender intended to pay. Senders of erroneously executed payment orders are entitled to "recovery from the [recipient] . . . to the extent allowed by the law governing mistake and restitution."[146]

(iii) Cancellation or Amendment of Transfers

Cancellation or amendment of electronic payment transactions creates additional verification problems. Although it contains requirements for documentation[147] and error resolution,[148] the EFTA is silent on these issues. In contrast, Article 4A has fairly elaborate rules. Article 4A requires verification of the cancellation or amendment if the sender and receiving bank have adopted a security procedure.[149] Article 4A also limits cancellation or amendment to cases in which the sender makes a mistake in the original payment order with regard to the amount or beneficiary, or to cases of unauthorized original payment orders.[150]

b. Delays Due to System Failure

System failures affect all electronic payments systems.[151] In the ordinary EFTA transaction, system failures are merely inconvenient: the customer

---

of the beneficiary, depending on the severity of the misdescription (non-existent or unidentifiable person or account, transfers in which the identifying name and account numbers do not correspond, person identified by name and account number with payment made to account number specified). U.C.C. § 4A-207 (1995).

[146]U.C.C. § 4A-205(a)(2)-(a)(3) (1995). Reference to the law governing mistake and restitution in Article 4A of course refers to common law rules for mistake and restitution. Rules for emerging retail electronic payments systems would require at the very least reconciliation of two groups of rules under the U.C.C.—respectively for Funds Transfers (discussed above) and for Negotiable Instruments (set forth in U.C.C. § 3-418 (1990)), as well as disparate state treatment of mistake and restitution. Rules governing mistake and restitution outside of the United States also would provide the basis for crafting appropriate rules for errors of this type. *See also*, Felsenfeld, *supra* note 13, at 564-65; Gerald Herrmann, *Background and Salient Features of the United Nations Convention on International Bills of Exchange and International Promissory Notes*, 10 U. PA. J. INT'L BUS. L. 517 (1988).

[147]15 U.S.C. § 1693d (1994).

[148]15 U.S.C. § 1693f (1994).

[149]U.C.C. § 4A-211(a) (1995).

[150]U.C.C. § 4A-211(c)(2) (1995).

[151]*See* KURTZMAN, *supra* note 7, at 179-83 (discussing systems failure in Fedwire, SWIFT, and CHIPS).

cannot get cash or complete any other transaction available on the ATM. In wholesale wire transfers, system failures are more problematic. For example, these failures pose risks of (1) potential breaches of the sender's duty to make timely payments, (2) recipient's loss of interest, and (3) recipient's inability to receive payments or settlements due.

In electronic cash transactions, system failures may cause both sets of problems associated with failed EFTA transfers and wholesale wire transfers. Accordingly, electronic cash transfers will require more specialized rules, such as those Article 4A provides,[152] to deal with their specialized failure problems. These problems include failures affecting the downloading of payment transfers, such as telephonic interruptions and failure of the electronic wallets to record the attempted transfer or to record it accurately.

c. Stop Payment or Reversibility of Payment

In addition to cancelling or contesting transfers, in certain cases, customers will expect that they can stop the downloading transfer to their electronic wallets or reverse the payment if the vendor does not perform. Rights and procedures under existing payments systems vary widely.[153] Differences in treatment of reversibility of payments in competing payments systems were at the core of the debate over the proposed New Uniform Payments Code in the late 1970's and early 1980's.[154] Because of the importance of finality of payment to Internet vendors, similarly significant disagreements over the scope of and procedures for stop orders and reversibility of payments in electronic cash transactions may arise.

---

[152]U.C.C. § 4A-305 (1995).

[153]Examples of these discrepancies include (1) the right to stop payment of checks by the payor bank under U.C.C. § 4-403 as long as the payor bank has a "reasonable opportunity" to act on the stop order before it pays or loses the right to act on the check as U.C.C. § 4-303 provides; (2) the limited right to reverse the payment under U.C.C. § 3-418; (3) the right to stop "pre-authorized transfers" under the EFTA so long as the consumer notifies the financial institution orally or in writing "at any time up to three business days preceding" the schedule date of the transfer under § 907(a) of the Act, 15 U.S.C. § 1693e(a); and (4) no right to "stop" under the federal Fair Credit Billing Act of 1974 ("FCBA"), 15 U.S.C. § 1666.

[154]New Uniform Payments Code Report, *supra* note 15, at 124-26.

d. Discharge of the Underlying Obligation; Determining when Payment Occurs

Payments systems must provide participants with certain general assurances. The obligor does not want to be required to pay twice for the same obligation. The obligee wants to ensure that the obligor will not be able to change its mind about the transaction and retrieve its funds after it has received the benefit of the exchange. Accordingly, both consumers and vendors, as well as any financial service provider representing either party in the transaction, need rules governing both discharge of the underlying obligation and the point at which payment occurs.

With regard to the discharge of the underlying obligation, neither of the two statutory consumer electronic payments systems laws, the EFTA or the FCBA, provide helpful models. Both Acts depend on the parties' underlying agreements to charge the consumer's account or to require the customer to pay charges that accrue on the account.[155]

In contrast, Section 4A-406 of Article 4A contains both sets of rules for wholesale wire transfers. First, subsection (a) establishes when payment is deemed to occur. This is the time at which the beneficiary's bank "accepts"[156] a payment order if the amount is equal to that which the beneficiary's bank accepted and not more than the amount of the originator's order.[157] Next, subsection (b) embodies the rule that has long characterized discharge: obligations are discharged by payment "to the same extent discharge would result from payment to the beneficiary of the same amount in money."[158] This subsection, however, does not discharge obligations in cases in which the obligor makes payment by a contractually prohibited means and the beneficiary suffers a loss that could have been avoided if the obligor had made the payment in accordance with the underlying contract, provided that the beneficiary notifies the obligor of refusal of payment and does not withdraw the funds or apply the funds to a debt.

---

[155]15 U.S.C. § 1693c (1994) (EFTA); 15 U.S.C. § 1637(a) (1994) (FCBA).

[156]U.C.C. § 4A-209(b) (1995) (defining when acceptance by beneficiary's bank occurs).

[157]See U.C.C. § 4A-406(c) (1995) for the rule governing payment orders equal to the amount of the originator's order less fees charged by intermediate banks in the transfer.

[158]*Cf.* U.C.C. § 3-310(b), (c) (1995) (covering negotiable instruments and giving discharge rules for uncertified checks, notes, and any other instruments aside from certified checks, uncertified checks, and notes).

Discharge rules for electronic cash transfers may need to distinguish between receipt of digitalized legal tender and receipt of private script. For example, receipt of private script might violate an express agreement between the buyer and the vendor.[159] In these cases, following Article 4A's approach, no discharge would occur if the vendor-beneficiary suffered a loss avoidable by a proper "tender" of payment.[160] In addition, if the payment does not result in discharge under Article 4A, the originator-obligor is "subrogated to the rights of the beneficiary to receive payment from the beneficiary's bank."[161] The amount of the payment received also could differ from the amount due under the contract because of the obligor's fraud,[162] or by diversion through error or fraud in the payment system.

Receipt of private script in systems such as DigiCash currently requires redeposit by the vendor into a bank before the value can be used for other purposes. Thus, receipt of electronic coins by the vendor is functionally different from receipt of a credit under Article 4A funds transfers in which the recipient of an Article 4A transfer has confidence that it will have "good

---

[159]This breach would be analogous to shipping goods "C.O.D." in transactions where the buyer has pre-paid the cost of the goods or the cost of shipment (U.C.C. § 2-320(1) (1995) (defining C.I.F. as including "the cost of the goods and the insurance and freight to the named destination")). Or it could be analogous to shipment under reservation (U.C.C. § 2-505(2) (1995) (considering a shipment under reservation one where the seller retains a security interest in the goods)).

[160]U.C.C. § 4A-406(b) (1993). Section 4A-406(b)'s "no discharge" is subject to four conditions:

> (i) [the payment was made] by a means prohibited by the contract of the beneficiary with respect to the obligation, (ii) the beneficiary, within a reasonable time after receiving notice of receipt of the order by the beneficiary's bank [advice of credit], notified the originator of the beneficiary's refusal of the payment, (iii) funds with respect to the order were not withdrawn by the beneficiary or applied to a debt of the beneficiary, and (iv) the beneficiary would suffer a loss that could reasonably have been avoided if payment had been made by a means complying with the contract.

[161]U.C.C. § 4A-406(b) (1995).

[162]Fraud by the obligor would be similar to fraudulent attempts at accord and satisfaction at common law. *See* Berger v. Lane, 213 P. 45 (1923) (discussing requirements and application of accord and satisfaction at common law). Revised Article 3 of the U.C.C. permits accord and satisfaction by use of a negotiable instrument only if the obligor tendered the instrument "in good faith" and as "full satisfaction" of the claim. U.C.C. § 3-311 (1995) (Accord and Satisfaction by Use of Instrument). The claimant must sustain other burdens of proof to obtain discharge. U.C.C. § 3-311 (1995).

funds'' either immediately or at the close of the business day.[163] Thus, the payee is more willing to tolerate an immediate discharge of the underlying obligation in an Article 4A transfer than in electronic cash transfers in which the vendor must convert the electronic value in order to use it outside of the electronic transfer system.

Discharge rules for electronic cash transfers also may require system rules for fee deductions by clearing or intermediary parties comparable to those in U.C.C. Section 4A-406(c).[164] Alternatively, the system rules may have to follow Article 4A's requirements that variations of its discharge rules may be made only by private agreements between transfer counter-parties.[165]

Although fees currently are rare, intermediaries in the new payments systems may begin to charge fees. To the extent that fees are not part of the original agreement between obligor and obligee, rules for new payments systems should be careful not to disturb the fee arrangements of the parties to the commercial transaction. The new rules might satisfy this goal by following the Article 4A standard of refusing to enforce system rules that vary the agreement of the individual parties to the transfer.[166]

2. Electronic Checks[167]

In terms of the types of reliability problems that may arise, electronic check transactions have elements of both existing paper-based checks and of retail and wholesale wire transfers. They will be similar to paper-based checks as ''pull'' transactions[168] and so require the payee to engage its bank

---

[163]For example, in Fedwire transactions the beneficiary receives Federal Reserve credits when the bank accepts the payment order. 12 C.F.R. § 210.31(b) (1995). In CHIPS transactions, the beneficiary bank receives a right to payment through CHIPS secured by collateral and due for settlement at the close of the business day. Knudson et al., *supra* note 1, at 270.

[164]U.C.C. § 4A-406(c) (1995).

[165]*See* U.C.C. § 4A-406(d) (1995) (''Rights of the originator or of the beneficiary of a funds transfer under this section may be varied only by agreement of the originator and the beneficiary.'').

[166]U.C.C. § 4A-406(d) (1995).

[167]Certainly some of the transfers will be ''checks'' drawn on or by banks and others will be ''drafts'' drawn on or by non-banks, such as insurance companies, buyers of goods, or issuers of traveller's checks. U.C.C. § 3-104(f)-(i) (1995).

[168]*See supra* text accompanying note 106.

in payment collection. They also will require "access devices" similar to those used in consumer electronic fund transfers or "security procedures" similar to those used in wholesale wire transfers.[169] Electronic checks raise numerous reliability issues, including transaction verifiability, delays due to system failure, stop payment and reversibility of payments, discharge of underlying obligations, and determining when final payment occurs.

a. Verifiability of the Transaction

To the extent that banks serve as the drawees of "electronic checks," the rules for verification of transactions may derive from those governing paper-based checks. As discussed above,[170] digital signatures or other validation devices[171] may substitute for the traditional requirement that the drawer sign the draw order. The combination of the validation device and record of the instruction should satisfy most of the likely payees in electronic check transactions.[172]

b. Delays Due to System Failure

Delays due to system failure are just as likely with electronic checks as they are with electronic cash, although the particulars of the failure may differ. Delays in receipt of the payment by the vendor may involve breaches of the underlying contracts to pay, whether based on a drawer's obligation to pay a draft under negotiable instrument law[173] or on the sales contract.[174]

---

[169]*See supra* text accompanying notes 128-32.

[170]*See supra* notes 92-117 and accompanying text.

[171]*See generally* PHYLLIS SOKOL, FROM EDI TO ELECTRONIC COMMERCE: A BUSINESS INITIATIVE (1995) (surveying use of electronic data interchange in different areas, including finance and electronic commerce).

[172]To ensure greater acceptance, rules for electronic checks could require express agreement of the vendor to be paid in this medium and allow for no discharge of the underlying obligation in cases in which the payment violated this agreement. *See* U.C.C. § 4A-406(b) (1995) (allowing discharge when four conditions are met).

[173]*See* U.C.C. § 3-104(a) (1995) (defining negotiable instruments as containing "an unconditional promise or order to pay a fixed amount of money"); U.C.C. § 3-414 (1995) (noting the obligations of a drawer on a draft).

[174]U.C.C. § 2-703 (1995) (noting seller's remedies in general expressly include as breach buyer's failure to make a payment when due).

Check collection in the United States depends largely on timely action by various parties. The process begins with the payee of the check,[175] moves to the depository bank and other collecting banks,[176] shifts to the payor bank,[177] and, in some cases, shifts back to the drawer.[178] Article 4 of the U.C.C. provides rules for timely action that relate to the necessity of making prompt presentment and of learning promptly if the payor has dishonored the check. Article 4 provides a defense to liability for delays "caused by interruption of communication or computer facilities, . . . [and] failure of equipment" only if "beyond the control of the bank" and if the bank "exercises such diligence as the circumstances require" after the interruption or failure ceases.[179] Furthermore, federal rules pertaining to check collection[180] also provide incentives for swift movement to and prompt return from the payor, or notice to the depository bank, in the event of dishonor.[181]

The tradition of imposing liability for these sorts of delays, at least in the United States, suggests that the rules for electronic checks should provide incentives for timely action and impose penalties for late action.[182] These rules should be similar to those in Article 4 so that they do not distort competitive balances between paper-based and electronic systems.

c. *Stop Payment or Reversibility of Payments*

Existing payments systems in the United States have radically different approaches to stop payment and reversibility of payments. For paper-based instruments, for example, the U.C.C. provides specialized rules governing stop payment orders of "items"[183] or account closings, including damages for failure to obey the customer's order on whose account the

---

[175]*E.g.*, U.C.C. §§ 3-302(a)(2), 3-304, 3-414(f) (1995).

[176]U.C.C. § 4-202(a), (b) (1995).

[177]U.C.C. §§ 4-301, 4-302, 4-303 (1995).

[178]*E.g.*, U.C.C. § 4-406 (1995) (Customer's Duty to Discover and Report Unauthorized Signature or Alteration).

[179]U.C.C. § 4-109(b) (1995).

[180]12 C.F.R. §§ 210, 229 (1995).

[181]*Id.*

[182]*E.g.*, U.C.C. § 4-302 (1995) (Payor Bank's Responsibility for Late Return of Item).

[183]U.C.C. § 4-104(a)(9) (1995). The definition of "item" covers "an instrument or a promise or order to pay money handled by a bank for collection or payment" but specifically excludes "a credit or debit card slip." *Id.*

item is drawn.[184] In addition, although finality of payment is a primary goal of the U.C.C.,[185] the U.C.C. has long provided for undoing final payment in the event of mistake on the part of the payor.[186] The U.C.C. limits the payor's opportunity to recover a payment made by mistake to those cases in which, among other things, the party receiving the payment did not act in good faith.[187]

For paper-based or electronic credit card transactions, the account holder's rights are more restricted. In the event of loss or theft, the account holder may report the incident to the card issuer and incur a maximum $50 fee for unauthorized charges to the card,[188] and also may close the account and obtain a new card. The customer, however, cannot make stop payment orders of the type Article 4 allows in which the account holder actually authorized the transaction but later determined that the payee has not performed. Instead, the account holder's primary recourse is through the less certain route of "error resolution" under the FCBA.[189] In addition, if a dispute concerning property or services purchased arises, the customer may withhold payment for the amount in dispute from the card issuer.[190] The FCBA restricts the nature of the investigation that the issuer must conduct. Consumer advocates have criticized the FCBA for affording inadequate protection for account holders who deal unintentionally with unscrupulous merchants.[191]

---

[184]U.C.C. § 4-403 (1995) (Customer's Right to Stop Payment; Burden of Proof of Loss).

[185]U.C.C. art. 4A pref. note (1995).

[186]U.C.C. § 3-418 (1995) (Payment or Acceptance by Mistake). Under this provision, "mistake" includes common law instances of mistake for which restitution is available as well as specialized mistake cases involving the drawee's mistaken belief that its customer had not stopped payment or its mistaken belief that the signature of the drawer was authorized. U.C.C. § 3-418(a)-(b).

[187]U.C.C. § 3-418(c) (1995).

[188]15 U.S.C. § 1643(a)(1) (1995).

[189]The Act's rules for error resolution require strict adherence to time schedules and requirement for notice to the card issuer. 15 U.S.C. § 1666 (1994), *as implemented by* 12 C.F.R. § 226.13 (1995).

[190]15 U.S.C. § 1666i (1994) (rights of credit card customers), *as implemented by* 12 C.F.R. § 226.12(c) (1995) (right of card holder to assert claims or defenses against card issuer).

[191]*See* Comment, *You May Have Already Won. . . : Telemarketing Fraud and the Need for a Federal Legislative Solution*, 21 PEPP. L. REV. 553, 570 (1994) (describing how telemarketers prefer payment by credit cards because of the long delay between the time they get paid and the customer gets the credit card bill so that customers usually do not

For debit card and other transfers governed by the EFTA, the customer's right to stop payment is limited to two situations. The first is "pre-authorized transfers" where the customer has given prior written authorization[192] and expects to make at least one transfer every 60 days.[193] The second involves cases in which the customer follows procedures set forth in the EFTA.[194] In addition, the customer has the right to error resolution under the EFTA. "Errors" for purposes of electronic fund transfers include: (1) unauthorized electronic fund transfers; (2) incorrect electronic fund transfers to or from the account; (3) omission from a periodic statement of an electronic fund transfer to or from the consumer's account that should have been included; and (4) computational or bookkeeping errors made by a financial institution.[195] Error resolution requires that the customer adhere to procedures similar to those required for resolution of credit card errors.[196] The EFTA limits consumer loss caused by unauthorized use to a minimum of zero dollars and a maximum of the total of the unauthorized transfers in the event that the account holder failed to notify the financial institution of the loss or theft and unauthorized transfers continued.[197]

Different standards for reversibility of payments created an uneven playing field among competing payments systems.[198] The Reporters of the proposed new Uniform Payments Code recommended repealing Articles 3 and 4 of the U.C.C. and federal laws governing payments systems "in order to establish a legal framework for all payments other than cash."[199] They also recommended adopting rules for stop payment orders and reversing

---

discover the fraud for several weeks leaving customers with remedies under the FCBA, 15 U.S.C. §§ 1601-1693r (1994)). *See generally* Federal Trade Commission, Revised Notice of Proposed Rulemaking: Telemarketing Sales Rule, 60 Fed. Reg. 30,406 (1995) (codified at 16 C.F.R. pt. 310 (1995)) (proposing, among other things, to make credit card laundering a violation of the telemarketing sales rule).

[192]12 C.F.R. § 205.10(b) (1995).

[193]12 C.F.R. § 205.10(a) (1995).

[194]These procedures are more fully set forth in Federal Reserve Board Regulation E, 12 C.F.R. § 205 (1995).

[195]12 C.F.R. § 205.11(a) (1995).

[196]12 C.F.R. § 205.11(d) (1995).

[197]15 U.S.C. § 1693g (1994).

[198]15 U.S.C. § 1693g (1994).

[199]*See* Introduction to New Uniform Payments Code Report, *supra* note 15, at 1 (explaining that "[t]he guiding philosophy . . . was that the new legal framework should not distort user choices among payment systems, e.g. as between checks and debit cards.").

final payments, including one that was designed for consumer transactions. Under the Committee's proposed Section 425, consumer drawers[200] would have had only three business days "from the time of the transaction either to stop or to reverse payments."[201] No party, however, could waive the right to stop payment on an unauthorized order,[202] if the drawer indemnified the financial institution against potential liability.[203]

To foster competition among new retail electronic payments systems, each system must adopt rules governing stop payments and reversibility of payment. Depending on customer tolerance (particularly in the United States), these rules may provide for waivers of these rights, so long as waivers are express between customer and system, and imposed on all parties to all transactions.

d. Discharge of the Underlying Obligation; Determining When Payment Occurs

Traditional check payment rules adopted the doctrines of merger and suspension to enforce the contract that the instrument embodied, particularly the requirements that the instrument "be payable on demand or at a definite time," and that the drawer of a check must pay if the drawee bank does not pay.[204] Discharge of a check depended on payment to a person entitled to receive payment, or to someone acting on such person's behalf.[205]

---

[200]New Uniform Payments Code Proposed § 425 (1982). Drawers other than consumers would waive the right to reverse payment on the order but would retain the right to stop payment under Subsection 425(9) "until the time the order is paid." New Uniform Payments Code Report, *supra* note 15, at 24-25. *See also* New Uniform Payments Code Proposed § 425 cmt. 2 (explaining that the proposed code "attempts to preserve and strengthen the value of stop payment orders for consumers" while also preserving the right of commercial parties to bargain differently); New Uniform Payments Code Proposed § 425 cmt. 3 (explaining the committee's objections to granting reversibility in electronic fund transfer transactions).

[201]New Uniform Payments Code Proposed § 425 (1982). Subsections (1) and (13) provided exceptions for cash withdrawals and orders that expressly waive the right to stop payment or reversal.

[202]New Uniform Payments Code Proposed § 425(9) (1982); New Uniform Payments Code Proposed § 425 cmt. 1 (1982).

[203]New Uniform Payments Code Proposed § 425(10) (1982).

[204]U.C.C. § 3-414(b) (1995).

[205]U.C.C. § 3-602 (1995).

Discharge of the check's underlying obligation depends on a variety of factors, including the nature of the check. For example, discharge of the obligation occurs when the obligee takes a certified check, cashier's check, or teller's check in payment of the obligation. In these cases, the discharge is equivalent to receipt of the amount of currency equal to the amount of the instrument.[206] When the obligee takes an uncertified check, discharge occurs when the obligor's bank pays or certifies the check.[207]

"Final payment" of paper-based checks may occur in several ways. These include: (1) payment in cash; (2) settlement of the check without a right to revoke the settlement under statute, clearing house rule, or agreement; and (3) failure to revoke a "provisional settlement" in the manner and time provided by statute, clearing house rule, or agreement.[208]

Because electronic checks may encompass all types of paper-based checks, electronic check systems will need protocols for discharge and final payment. The payment system may adopt corollary rules for presentment, dishonor, and notice of dishonor similar to those of U.C.C. Articles 3 and 4.[209]

B. Security Rules

Despite considerable attention from Internet standards groups and software manufacturers,[210] security for new retail electronic payments systems remains a concern. If these payments systems had reliable security in place to guard against interception of sensitive information, such as credit card validating information, system rules for security could be limited. During this introductory phase, however, commercial needs may require more protection than currently exists. As each system perfects its security measures

---

[206]U.C.C. § 3-310(a) (1995).

[207]U.C.C. § 3-310(b)(1) (1995).

[208]U.C.C. § 4-215 (1995).

[209]The payment system may adopt these rules such as those in U.C.C. Articles 3 and 4 as clearing house rules or system agreements. Alternatively, the payment system could adopt rules based on U.C.C. Article 4A's rules for finality, U.C.C. § 4A-406 (1995).

[210]*E.g.*, Netscape, *supra* note 50; RSA Data Security, Inc., Major Networking and Messaging Vendors Endorse Open Specification for Secure E-Mail, *available at* http://www.rsa.com/pub/S-Mine/announcement.txt (July 24, 1995) (describing new security protocol for text-based messages and other commercial applications).

(assuming its feasibility),[211] it may be possible either to relax security rules or to tolerate wider variations of the rules adopted by individual participants in the payments systems.[212]

Security issues for purposes of this Article encompass risks from third parties, as opposed to risks that one of the counter-parties will not perform as agreed. Third party risks include new subcategories of conversion: (1) unauthorized orders to download or to pay; (2) alterations either of the amount contained in the instruction/payment or of the person entitled to payment; and (3) theft or waylaying of the payment instruction or receipt of payment. Security rules should require procedures for obtaining records and for closing accounts. These functions provide particularly important protections when evidence of either account penetration or unauthorized use of an aspect of the account, such as account number, personal identification number, or digital signature, exists.

Protections against enforcement of unauthorized transactions will be a significant factor in gaining customer acceptance of new retail electronic payments systems. The need for security procedures and legal standards may be greater for Internet-based payments mechanisms than for non-Internet stored-value payments mechanisms.

1. Electronic Cash—Unauthorized Use and Other Concerns

Despite security precautions, electronic cash systems are theoretically susceptible to the risk of unauthorized use. Security risks exist at all three points at which the access device is used in electronic cash transfers. At the first step in an electronic cash transaction, an interloper might divert value as the account holder attempts to download value from the depositary account, intercept the account holder's address and identifying information, or order additional downloading without the account holder's authorization. The account holder whose account is debited without authorization should have a means of protecting against such interceptions and of recovering the misappropriated funds. During the second step, when

---

[211] *See* Sandberg, *supra* note 40, at B8 (suggesting that security flaws may continue); *see also* Carley & O'Brien, *supra* note 40, at A1 (explaining penetration of Citicorp's cash management wholesale wire transfer systems).

[212] Essentially, these security issues relate closely to pricing considerations.

the account holder transfers value to a vendor, unscrupulous vendors, or their embezzling employees, could program their systems to take more than the amount required for the purchases.[213]

Despite attempts by systems such as DigiCash to limit "electronic coins" to a single use and to guard against the possibility of counterfeiting,[214] a committed interloper may gain access even to the more sophisticated electronic systems.[215] Accordingly, rules must govern unauthorized use, especially for payments systems in which transactions will be very difficult to reconstruct.[216]

Models for these rules raise some of the same issues associated with "reliability rules."[217] For example, rules governing unauthorized use provide assurance that (1) the person requesting the transaction is either the customer or the customer's authorized agent, using techniques such as digital signatures or personal identification codes; (2) the customer's access device was not lost or stolen; and (3) that the recipient is the intended payee. Article 4A uses the "security procedure" as the gateway for wholesale wire transfers;[218] it requires that the security procedure be established by agreement between the customer and receiving bank[219] and that it be "a commercially reasonable method of providing security against unauthorized payment orders" as a matter of law.[220] Article 4A also recognizes agreements

---

[213]Such an unauthorized transfer is analogous to the vendor who makes more than one impression of a credit card or whose employees take impressions for later, unauthorized uses or to create counterfeit cards.

[214]*See supra* text accompanying notes 128–166.

[215]*See also* John Markoff, *The New Watchdogs of Digital Commerce*, N.Y. TIMES, Oct. 16, 1995, at D1, D10 [hereinafter *Watchdogs*]; John Markoff, *Discovery of Internet Flaws is Setback for On-Line Trade*, N.Y. TIMES, Oct. 11, 1995, at A1, D3 [hereinafter *Setback*].

[216]For example, DigiCash's "ecash" system restricts information about the customer's ecash password to the customer. Accordingly, the bank from which funds are downloaded may have information that it debited the customer's account and the amount of the debit and the alleged recipient (DigiCash), and the access device used to obtain the funds.

[217]*See supra* text accompanying notes 130–209.

[218]U.C.C. §§ 4A-201 (1995) (Security Procedure), 4A-202 (1995) (Authorized and Verified Payment Orders).

[219]U.C.C. § 4A-201 (1995) (rejecting comparison of a signature on a payment order or communication with the specimen signature of the customer as a sufficient procedure for this purpose).

[220]U.C.C. § 4A-202(b), (c) (1995). Factors with which to determine whether the security procedure utilized meets the test of "commercial reasonableness," include:

> [T]he wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally

in which the customer agrees to be bound by payment orders processed according to the security procedure the customer has selected.[221]

To protect against unauthorized use, the EFTA requires both an access device and personal identification number.[222] Credit card transfers rely on the presentation of the card, comparison of the signature on the card with that of the customer presenting the card, and, in most cases, express electronic authorization obtained from the card issuer. Each of these models that protect against unauthorized use will serve some part of the emerging electronic payments systems.

2. Electronic Checks—Unauthorized Orders and Fraudulent Alterations

Electronic checks and drafts arguably present fewer security risks than existing paper-based payments, at least in the United States.[223] The theoretical risk that an interloper will divert the order to pay and succeed in obtaining payment appears to be smaller than in the paper-based systems, largely because the delivery mechanisms may be more secure than hand-

---

issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated.

U.C.C. § 4A-202(c) (1995). Given the current concerns about security procedures in place for certain electronic payments systems, we should be very cautious about adopting a standard at this time that presumes adequacy of the security procedures based on "general use" and "similarly situated" parties. These standards, however, reflect the approaches taken in Articles 3 and 4 of the U.C.C. for paper-based payment systems.

[221]U.C.C. § 4A-202(c) (1995). One problem with customer selection of security procedures is the relative ignorance in the customer base vis-a-vis the industry of the range of security flaws in the system. *See Watchdogs*, *supra* note 215, at D10 ("[N]ewly publicized" flaws in Netscape software "were generally known among software engineers who have developed and maintained the Internet since its creation more than 25 years ago"; tradition of "unfettered inquiry and curiosity" about Internet and software security "grated against more conservative business cultures that wanted to keep information about computer security a closely guarded secret").

[222]*See* 15 U.S.C. § 1693g(a) (1994) (predicating consumer liability on presence of access device and additional method of identification).

[223]Individuals and organizations in the United States use many-fold more checks and drafts than do their counterparts in similarly developed nations. *See* DEVELOPED COUNTRIES' PAYMENT SYSTEMS, *supra* note 20, at 106, 150, 226, 249–250 (providing figures regarding use of paper-based instruments).

or mail-delivery.[224] However, opportunities for customers and banks to detect a diversion before payment and to identify the culprit appear to be smaller in an electronic payments system. As a result, electronic checks will require rules governing unauthorized use, as well as a means to prevent and distribute the loss.

Three primary U.S. models serve as samples for developing new rules: Articles 3 and 4 of the U.C.C. for paper-based orders to pay, Article 4A for wholesale wire transfers, and the EFTA for electronic fund transfers. In addition, state laws that provide for the registration and verification of digital signatures, such as Utah's Digital Signature Act,[225] offer guidance about appropriate means of protecting against unauthorized transactions.

Because the EFTA places dollar limits on liability for unauthorized use and rules for paper-based checks do not, rules for electronic checks may adopt features of regulatory schemes for wholesale wire transfers, paper-based checks, and electronic fund transfers for guidance. We also have presumptions—at least in the United States—that the party who was in the best position to prevent the loss should bear the loss. Accordingly, electronic check transactions should include rules such as Section 4A-203 that governs funds transfers that passed muster under the agreed-upon security procedure, but that in fact were not authorized customer orders. Article 4A sets forth two means of handling these cases that would apply to the electronic check transaction. First, banks and customers could have express written agreements under which the electronic check drawee bank would limit its ability to enforce the check or to retain payment previously received from the customer.[226] Second, the customer could have the opportunity to prove that the particular electronic check was not transmitted by a person entrusted or authorized to act and that the check issued in breach of the security procedure established by the bank and customer for electronic checks drawn on the account.[227]

---

[224]*See Major Banking-Computer Consortium to Develop Electronic Check; FSTC promises early demonstrations using the Internet*, BUS. WIRE, Aug. 23, 1995, *available in* LEXIS, Nexis Library, CurNWS file (electronic checkbooks, digital signatures, and delivery by Internet or "other electronic highway" rendering electronic check "virtually impossible to forge" and verifiable against alteration).

[225]UTAH CODE ANN. §§ 46-3-101 to 46-3-504 (1995).

[226]U.C.C. § 4A-203(a)(1) (1995).

[227]U.C.C. § 4A-203(a)(2) (1995).

The rules governing electronic checks also could borrow procedures from the EFTA and from U.C.C. Articles 4A and 4 regarding time limits on recovery when the customer did not act with reasonable promptness in notifying the bank of the suspected unauthorized transaction.[228] Finally, the New Uniform Payments Code proposal provides other useful models for verifying the identity of the transmitter of the electronic check or draft.[229]

In addition to rules for verifying authority to conduct the transactions and for guarding against unauthorized use, electronic check systems will require rules for loss distribution in the event of fraudulent alteration. Currently, Section 3-407 of the U.C.C. provides these rules for paper-based instruments. Under this Section, the obligation is discharged if the payee fraudulently alters the instrument.[230] However, it also protects certain parties, primarily those who have relied on payment, from total loss of the benefit of the payment by permitting enforcement of the original terms of the instrument.[231] In the case of instruments altered by unauthorized completions, enforcement would occur on the terms as completed.[232] Article 4A treats alterations either as erroneous executions if the amount exceeded that established in any security procedure[233] or as unauthorized payment orders.[234] The model for electronic check transactions may require features of the rules in Articles 3 and 4A.

Reliability and security rules for new retail electronic payments systems can draw upon models provided by existing retail and wholesale payments systems, including electronic fund transfers, wholesale wire transfers, (retail) credit cards, and checks. New retail payments systems—not subject to existing statutory or clearing house rules, or to contracts with existing customers—may alter their initial rules as the electronic payments industry as a whole, or any particular payments system, devises more tamper-proof

---

[228]15 U.S.C. § 1666(c) (1994) (60-day-cap); 12 C.F.R. § 205.6(b)(2) (1995) (60 day cap); U.C.C. § 4A-205(b) (1995) (90 day maximum reasonable time); U.C.C. § 4-406(d), (f) (1995) ("reasonable time" not exceeding 30 day and one-year limitations on recredits).

[229]*See generally* New Uniform Payments Code Proposed §§ 412(5), 508-509, 511 (establishing transmitter verification requirements).

[230]U.C.C. § 3-407(b) (1995).

[231]U.C.C. § 3-407 (1995).

[232]U.C.C. § 3-407(c) (1995).

[233]U.C.C. § 4A-205 (1995).

[234]U.C.C. § 4A-202 (1995).

methods of guaranteeing reliability and security to participants. Choice of legal models will influence how emerging systems will compete with other existing and emerging systems and the manner in which innovation will occur.

IV. WHY A STANDARD AT THIS TIME?

Traditionally, rules for new payments systems have emerged as problems that required resolution arose. A prime example of this type of development is evident in the law governing wholesale wire transfers. From approximately 1918 until the adoption of Article 4A, no comprehensive law governed these transfers.[235] Instead, wholesale wire transfers operated under a combination of rules adopted by funds transfer systems, Federal Reserve Board regulations relating to Fedwire transactions, and individual contracts.[236]

The absence of a comprehensive statutory scheme until the early 1990's did not unduly hinder wholesale wire transfers for three reasons. First, participants in the funds transfer often had long-established relationships with each other that caused them to work to preserve their relationships. Similarly, parties to the underlying transactions (sales, check-clearing, foreign exchange, federal funds) had relationships as well. As a consequence, this patchwork legal framework did not present as many opportunities for disputes as are likely to arise under new retail electronic payment mechanisms where counter-parties are less likely to know each other.

Second, the club-like environment of wholesale funds transfers allowed resolution of most disputes on the basis of "gentlemen's agreements."[237] Third, because unresolved disputes involved very large sums of money, disputants under wholesale funds transfer systems were more likely to have, or be able to attract, counsel to resolve disputes.

In contrast, retail electronic payments systems may need the benefit of baseline rules in order to foster and maintain acceptance among potential

---

[235]U.C.C. art. 4A pref. note (1995).

[236]Scott, *supra* note 18, at 1668–78. *See also* Robert G. Ballen & Natalie H. Diana, *The Need for Article 4A*, 45 BUS. L. 1399, 1399 (1990).

[237]*See* Scott, *supra* note 18, at 1678.

customers. One payments system expert suggested several reasons to adopt an early comprehensive regulatory scheme:

> Why should people care about how some extremely technical payments system disputes are settled? The reason is that they relate directly to the way that bank-like services can, and will, be transferred from payor to payee. They impact on retail pricing for consumers and, equally important, on the manner and kinds of money services available to the public. Furthermore, unless and until the private parties can amicably agree on basic responsibilities, the electronic payments modes may not be fully utilized. Because of the risk of costly litigation, adoption of the new payments technology through joint ventures may be slowed. *The expected consumer benefits of all the scale economies may fail to be realized fully.*[238]

Additional reasons support the conclusion that rules governing electronic payments systems should be adopted at this time. First, new payments systems, particularly those radically different in form from existing systems, do not fit easily into the rules for existing systems. As a result, the rules that evolve may not provide adequate protection for customers of the new payments system.[239] Adequate customer protection rules would foster wider acceptance of these technologies in lay circles and spur additional Internet or smart-card commercial developments.[240]

Second, adoption of rules (particularly if they apply across national borders) may avoid or reduce disparities in regulation between both national and local jurisdictions otherwise likely to exist or arise in the short-term.[241] They also would reduce differences in regulatory pace and style, as opposed to content, that typically act as a drag on innovation.

---

[238]Elinor Harris Solomon, *Conflicts: Banks, Consumers, and the Law*, in ELECTRONIC MONEY FLOWS—THE MOLDING OF A NEW FINANCIAL ORDER 157 (Elinor Harris Solomon, ed. 1991) (emphasis added).

[239]*See* Note, *Consumer Protection and Payments Systems: Regulatory Policy for the Technological Era*, 98 HARV. L. REV. 1870 (1985) (focusing on proposed New Uniform Payments Code that emerged, in part, as Article 4A and in revisions to Articles 3 and 4 of the U.C.C.).

[240]*See* Jeff Benjamin, *IRE Drafting an "Electronic Check" Product of Baltimore Firm's Research Debuting on Internet*, THE DAILY RECORD, Aug. 30, 1995, at 3 (citing John Bowers, executive vice president of the Maryland Bankers Association, on need for complex safeguards before general public will put "real money" on the open wire).

[241]*See* Felsenfeld, *supra* note 13, at 60 (noting that differences existed in positions among U.S. and foreign delegations to UNCITRAL drafting group).

Third, rules governing the new payments systems may occupy terrain that other regulatory "models," such as law enforcement and monetary policy otherwise might dominate. Rules for payments systems based solely on law enforcement or monetary policy models would shape the industry's future paths very differently.[242]

Fourth, early rules might avoid "backlash" regulations. Article 4A, although not adopted as early as the rules advocated in this Article, developed without suffering the backlash of the federal Truth in Lending Act[243] or the federal Fair Debt Collection Practices Act.[244] Congress promulgated both Acts as attempts to address the imbalance between consumer interests and providers that engaged in abusive or misleading conduct.[245]

Fifth, because of the lack of ties between Internet-payments participants and the large volume of expected transactions, disputes undoubtedly will arise. Disputes without legal frameworks cost more to resolve and are more likely to be resolved haphazardly.[246] The paucity of rules increases the risks faced by parties to these payments transactions.[247]

Sixth, because drawers or payors and payees in Internet purchase and payment transactions will not deal face-to-face, an "unregulated" or ineffectively regulated payments system is more likely to invite opportunities

---

[242]Rules based on such models also would break with tradition in the regulation of payments systems in which operational rules precede others (*e.g.*, Article 4A and the Treasury's 1995 record-keeping and "travel" requirements for (wholesale) funds transfers and funds transmittals). *See* U.C.C. art. 4A pref. note (1995); 31 C.F.R. § 103 (1995). This is not to suggest that specialized considerations for law enforcement and monetary policy will not be required as these new retail systems progress.

[243]15 U.S.C. §§ 1601-1667 (1994).

[244]15 U.S.C. §§ 1692-1692(o) (1994).

[245]The federal Truth in Lending Act ("TILA") certainly was a reaction to problems evident in the marketplace. For example, Section 102 of TILA provided:

> (a) [I]t is the purpose of this title to assure a meaningful disclosure of credit terms so that the consumer will be able to compare more readily the various credit terms available to him and avoid the uninformed use of credit, and to protect the consumer against inaccurate and unfair credit billing and credit card practices.
>
> (b) The Congress also finds that . . . leases [for consumer use] have been offered without adequate cost disclosures. It is the purpose of this title to assure a meaningful disclosure of the terms of leases of personal property for personal, family, or household purposes so as to enable the lessee to compare more readily the various lease terms available to him, limit balloon payments in consumer leasing, enable comparison of lease terms with credit terms where appropriate, and to assure meaningful and accurate disclosures of lease terms in advertisements.

[246]Scott, *supra* note 18, at 1664.

[247]Scott, *supra* note 18, at 1664.

for fraud.[248] Finally, because these Internet-payments systems will probably carry a high volume of low-dollar-value transactions or may involve cross-border participants, the legal system will have diminished capacity to deal with these errors and disputes without standardized rules.

V. WHY AN INTERNATIONAL STANDARD?

Existing and planned electronic financial transactions have major growth implications for the global economy.[249] Experts predict a burgeoning market for Internet-based information services and other commercial offerings.[250] But, as one commentator observed, "the Internet is no more controlled by the United States than is the United Nations."[251]

To the extent that new retail payments systems remain without adequate legal standards, commentators predict that customers' acceptance of some forms of electronic financial transactions could be slower than would be the case with adequate participant protection.[252] In addition, experts recognize a need to level the playing field among bank and non-bank financial service providers. This would aid in the development of the technology necessary to implement these electronic financial transactions.[253]

An international standard would avoid costs associated with disparate local regulation, including dampers on innovation that result from excessive or inconsistent regulations adopted by different jurisdictions.[254] In addition, because electronic financial transactions are or may be regulated by some

---

[248]*See* Antilla, *Has Cyberspace Got a Deal For You!*, *supra* note 4, § 3 (Money & Business/Financial Desk), at 5 (SEC action on fraud on Internet). Internet features such as "anonymous re-mailing" will complicate the identification of the miscreant and the resolution of disputes. *See generally* Peter Sinton, *VISA Wants to Kill Cash; It Hopes 'Smart Cards' Will Become the Payment Method of Choice*, S.F. CHRON., Oct. 11, 1995, at B1; Robert Hurtado, *Treasury Prices Fall Again, Dollar's Decline Is Cited*, N.Y. TIMES, Oct. 24, 1995, at D26 (describing possible agreement between U.S. and Japan to swap Treasury securities to help Japanese banks manage possible cash crisis).

[249]KURTZMAN, *supra* note 7.

[250]Powell, *supra* note 46.

[251]Peter Lewis, *On the Net: Privacy for Computers? Clinton sets the stage for a debate on data encryption*, N.Y. TIMES, Sept. 11, 1995, at C5.

[252]*See supra* note 122 and accompanying text.

[253]*E.g.*, 1992 OTA PAPER, *supra* note 2, at 2.

[254]For a discussion of these costs from the perspective of differing state product quality laws in the United States, see David A. Rice, *Product Quality Laws and the Economics of Federalism*, 65 B.U. L. REV. 1 (Jan. 1985).

nations and not others, the market may seek the lowest common regulatory denominator.[255] However, in so doing, the market would risk losing public acceptance as problems arise. For this reason, banking commentators urge development of international standards.[256]

The Uruguay Round of the General Agreement on Tariffs and Trade ("GATT") spurred new opportunities for international financial transactions.[257] Subsequent World Trade Organization agreements on cross-border financial transactions (to which the United States is not a party) and increasing "border-less" financial transactions involving exchange and securities,[258] suggest that only international legal standards suit the tasks ahead.

VI. WHY SELF REGULATION?

The question of who will regulate new retail electronic payments systems is one of the major issues facing the infant electronic payments systems. This debate is tied to the question of whether governments or private organizations should control the Internet. Some commentators argue that government regulation of the Internet would "act as a drag on commerce,"[259] and, hence, advocate private regulation.[260]

Unlike the development of standardized rules, there are six reasons supporting a fairly long delay in promulgating new regulations. First, many

---

[255]*Id.* at 44-45.

[256]*E.g.*, J. Duffy, *Global Approach Argued to Protect Consumer in Electronic Banking*, AM. BANKER, July 18, 1988, at 2.

[257]General Agreement On Tariffs and Trade—Multilateral Trade Negotiations (The Uruguay Round): Agreements on Trade In Goods 33, International Legal Materials (The Am. Soc'y for Int'l Law) 28 (1994).

[258]Peter Truell, *A Japanese Bank Is Indicted in U.S. and Also Barred*, N.Y. TIMES, Nov. 3, 1995, at A1.

[259]*Internet Protection Proposed; House Panel Wants to Freeze FCC Budget for FY 1996*, COMMUNICATIONS DAILY, June 20, 1995, 1995 WL 6459914.

[260]One risk of private rules is that the rules will exclude new entrants and, so, may chill innovation. Commentators have explored these issues in connection with shared electronic fund transfer and credit card networks. *E.g.*, David S. Evans & Richard Schmalensee, *Economic Aspects of Payment Card Systems and Antitrust Policy Toward Joint Ventures*, 63 ANTITRUST L.J. 861 (1995); Dennis W. Carlton & Alan S. Frankel, *The Antitrust Economics of Credit Card Networks: Reply to Evans and Schmalensee Comment*, 63 ANTITRUST L.J. 903 (1995).

jurisdictions already supervise the bank and non-bank service providers that will offer new retail electronic payments services. Second, as described above, statutory or regulatory legal standards for payments systems traditionally have lagged behind implementation by some period.[261]

Third, there is a trend toward private regulatory schemes for globally accessible industries.[262] Fourth, effective private groups serving Internet-based industries are emerging.[263] Indeed, in light of the "civil libertarian ethos of the Net,"[264] it is possible that Internet participants would have more respect for private rules than for regulations promulgated by governments.

Fifth, given the extensive variety of potential payments mechanisms that fall under the rubric of "retail electronic payments systems," regulations, as opposed to rules, would face obstacles in keeping pace with change. In addition, because of its associational, payment-system-rule character, the private-rule approach may facilitate adaptation to changes in the technology that pertain to individual aspects of the initial standards. Finally, experts recognize that international cooperation among industry members may help to "find solutions to shared problems such as standards development, systems failure, or security risks."[265]

---

[261]Examples of this pattern in the United States include the EFTA (enacted in 1977, following introduction of bank ATM cards in the late 1960's and early 1970's), and Article 4A (1990 adoption for system running from at least 1918).

[262]For example, the World Administrative Radio Conference allocates frequencies globally. Other examples of self-regulation that appear to work in complex commercial contexts include the International Small Satellite Organization, and the Intelsat Assembly of Parties, beginning in the mid-1960s, on the international scale. *Intelsat meeting could be landmark gathering; pricing structures separate systems issues on agenda*, BROADCASTING, July 29, 1985, at 4, *available in* LEXIS, Market Library, ASAP II File. Other examples include the National Futures Associations and the National Association of Securities Dealers ("NASD") on the domestic side. *Id.*

[263]Among these groups are the World Wide Web Consortium based at the Massachusetts Institute of Technology, the Platform for Internet Content Selection ("PICS"), the Internet Society, and the Internet Engineering Task Force ("IETF"). *See* Steve Lohr, *Industry Seeks Means to Filter Internet Content*, N.Y. TIMES, Sept. 11, 1995, at C5. PICS was formed to provide private-sector alternative to government censorship of Internet for pornography and development of private blocking software. For information on the IETF, see IETF Overview, *available at* ftp://ds.internic.net.ietf/lietf-dscription.txt.

[264]Lohr, *supra* note 263, at C5 (quoting Rob Glaser, a software executive who will lead the PICS group).

[265]1992 OTA PAPER, *supra* note 2, at 4.

VII. CONCLUSION

This Article advocates prompt adoption of international rules that would govern the operation of emerging retail electronic payments systems, particularly digital cash and electronic checks. International rules based on agreements by providers of payments systems (as opposed to regulations promulgated by governments) offer greater opportunity to gain acceptance from potential customers. International rules also offer greater flexibility to respond to technical innovations in these systems. This rule-based approach focuses on *like products* or activities rather than on *like institutions* and, accordingly, offers a level playing field for entities offering competitive products.

A rule-based approach would accept the invitation imbedded in the U.S. payments systems laws to vary normal relationships by agreements of parties or by "clearing house" or associational rules.[266] It also would avoid the lengthy processes of creating and amending statutory schemes for systems that are changing rapidly. Finally, competition would force the members of these associations to develop user-friendly rules or risk losing business to other payments systems.

This proposal would not substitute private rules for all aspects of existing "regulatory" functions. Rather, it would leave in place existing supervisory authority that focuses on the institutional character of the service provider for purposes of safety and soundness and monetary policy.[267] These supervisory institutions may be at the national or state or provincial levels. This proposal recognizes that a new regulatory authority for globally accessible retail electronic payments systems may become necessary in the future.

A collateral benefit of this "leave-them-where-they-are-regulated" attitude would inure to institutions, such as banks, with reputations as trustworthy enterprises. Other brand-name providers of competing products (such as AT&T, Visa International, MasterCard, American Express, Thomas Cook, and First Data Corp.) could rely on their brand names to market their products. Still others (such as postal and transit authorities

---

[266]*See e.g.*, U.C.C. §§ 4-103, 4A-501 (1995) (providing that agreement-based rules should restrict variation by customer agreement only where current payments systems practices or regulatory systems would restrict such variations).

[267]Accordingly, banks, non-bank financial institutions, and non-bank corporations would be regulated by their current supervisory authorities for these new purposes.

in western Europe and the United States) would have the marketing advantages of quasi- or full-governmental status behind their products. Finally, new service providers whose products lack brand-name recognition, such as DigiCash and Mondex, could enter into joint ventures with trusted parties, such as banks, other major financial services providers, or other trusted brand names, to achieve a competitive edge.

Legal standards for emerging retail payments systems can draw upon standards that have been developed for existing retail and wholesale electronic payments systems (electronic fund transfers, credit cards, and wholesale wire transfers), as well as for paper-based payments systems (negotiable instruments such as checks, and paper-based credit card transactions). Existing laws governing payments systems often impose different standards on competing payments systems. Emerging payments systems appear to have features of more than one of the existing systems. Accordingly, in developing legal standards for emerging systems, we must evaluate the similarities and differences in the systems and their relationships to existing systems. In addition, we must consider how the choice of legal standards for emerging electronic payments systems will affect competition between systems and prospects for innovation.

Each of the proposals in this Article will turn on the manner and pace with which these new retail electronic payments systems develop. That development is inextricably entwined with customer acceptance. Accordingly, emerging payments systems should reject the anarchical tendencies of the Internet community, acknowledge problems with security that industry members currently can offer, and adopt baseline protections and adjust them as quickly as experience allows. If the emerging payments systems do not, the industry takes the risk of having more onerous, and potentially less functional, standards imposed by local, national, and international authorities.