Chicago-Kent College of Law
Scholarly Commons @ IIT Chicago-Kent College of Law

All Faculty Scholarship | Faculty Scholarship

March 1996

Legal and Technological Infrastructures for Electronic Payment Systems

Henry H. Perritt Jr.
IIT Chicago-Kent College of Law, hperritt@kentlaw.iit.edu

Follow this and additional works at: https://scholarship.kentlaw.iit.edu/fac_schol

 Part of the Internet Law Commons

Recommended Citation

Henry H. Perritt Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 Rutgers Computer & Tech. L.J. 1 (1996).
Available at: https://scholarship.kentlaw.iit.edu/fac_schol/473

This Article is brought to you for free and open access by the Faculty Scholarship at Scholarly Commons @ IIT Chicago-Kent College of Law. It has been accepted for inclusion in All Faculty Scholarship by an authorized administrator of Scholarly Commons @ IIT Chicago-Kent College of Law. For more information, please contact jwenger@kentlaw.iit.edu, ebarney@kentlaw.iit.edu.

LEGAL AND TECHNOLOGICAL INFRASTRUCTURES FOR ELECTRONIC PAYMENT SYSTEMS

HENRY H. PERRITT, JR.*

---

* Henry H. Perritt, Jr., is Professor of Law at Villanova University School of Law and President of the Villanova Center for Law & Policy. He is a member of the bars of Virginia, Pennsylvania, the District of Columbia, Maryland, and the United States Supreme Court. He can be reached by phone at (610) 519-7078, by fax at (610) 519-7033, and on the Internet at perritt@mail.law.vill.edu or at perritt@law.vill.edu. The author wishes to thank Charles Merrill, a partner in the law firm of McCarter and English, for his suggestions and comments, as well as Brian P. Crowner, Paul Boltz, and Martin Noonan, Class of 1996, Villanova University School of Law, for their research and brainstorming assistance. Mr. Noonan's contributions as a source checker were particularly significant. The author also wishes to thank his long-time friend, Michigan and Ohio banking attorney Michael H. Shaut, who provided suggestions from a banking law perspective.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 1 1996

I. INTRODUCTION

Commercialization of the Internet offers merchants and consumers access to the Internet's worldwide market.[1] Greater commercialization depends, however, on the establishment of a reliable and efficient method of payment. Economic transactions on the Internet will have to be at least as transparent, convenient, and secure for consumers and merchants as ordering merchandise by telephone with the use of a credit card.[2]

The use of telephone credit card transactions as the benchmark for an Internet payment system suggests that the most obvious model for Internet payments is credit cards. Unfortunately, most consumers are reluctant to transmit their credit card numbers over the Internet.[3] A method for ensuring privacy on the Internet[4] as

---

1. *See Is There Gold in the Internet?*, ECONOMIST, Sept. 10, 1994, at 73-74 (estimating Internet users at 20 million worldwide and user growth at more than one million per month).

2. As currently used by most mail order credit card operations, the telephone system secures privacy better than the Internet, but does not provide better authentication security. *See infra* text accompanying notes 170-84.

3. *Is There Gold in the Internet?*, *supra* note 1, at 74. This reluctance is based mostly on myths and hysteria that have pervaded the Internet community. *Id.* For a discussion of the technical risks involved in transmitting credit card numbers over the Internet, *see, e.g.*, Charles Arthur, *Crime Gangs use Internet to Access Credit Card Fraud*, INDEPENDENT-LONDON, June 2, 1995, at 3; Talila Baron, *Safer Than you Think*, COMM. WK., June 12, 1995, at 57; R.J. Ignelzi, *Stolen Identities: Unwary Consumers Find Credit Ruined as Crooks go High-Tech*, SAN DIEGO UNION-TRIB., July 2, 1995, at D1; Martin F. Noonan, *An Analysis of the Security Risks Involved in Transmitting Credit Card Numbers Over the Internet* (Oct. 18, 1994) (unpublished white paper on file with Villanova Center for Information Law and Policy) (providing an insightful comparison of the technical risks involved in transmitting credit card numbers over the Internet and over the telephone system).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 2 1996

well as an authentication system[5] must be developed to overcome this reluctance.

Another way to facilitate commerce on the Internet is to use digital cash ("cybercash").[6] Cybercash offers several features that make it an attractive alternative to credit card payments over the Internet. For example, cybercash is convenient, easy-to-use, and may not require third-party authorization before it can be used for a purchase.[7] Cybercash can also be implemented so as to permit anonymous use, thereby avoiding the transactional records that conflict with the personal privacy preferences of many credit card users.[8]

Cybercash systems tend to become indistinguishable from

---

4. Privacy is necessary to prevent credit card numbers from being intercepted by potential forgers. The credit card industry surpassed the two billion dollar loss-mark in 1985, reaching almost 31 of the combined MasterCard and VISA credit card suppliers that year. Jeffrey Kutler, *Smart Cards: How Bright are They?*, AM. BANKER, July 7, 1986, at 1.

5. Authentication is a process for verifying a credit card transaction. It is composed of two elements. First, the merchant must verify that the credit card account has a balance and credit limit sufficient to cover the transaction. Second, the merchant must determine whether the owner of the credit card account authorized the transaction.

6. Digital cash is also referred to as electronic money, electronic cash, or, more colloquially, as "cybercash." *See* CROSS-INDUSTRY WORKING TEAM, *Electronic Cash, Tokens and Payments in the National Information Infrastructure*, § 1.3 (Sept. 1994) (available on the Internet at http://www.cnri.reston.va.-us:3000/XIWT.public.html). The Cross-Industry Working Team (XIWT) is a "membership organization consisting of a diverse group of communications, computer system, information and service providers who have joined together to develop a common technical vision for the National Information Infrastructure (NII)." *Id.* XIWT issued a report that examined the design and legal considerations involved in implementing a digital cash payment system. *Id.* at § 1.2; *see also* Amy Cortese & Kelly Holland, *What's the Color of Cybermoney?*, BUS. WK., Feb. 27, 1995, at 80-81 (describing interest by banks and credit card issuers in electronic payment systems for the Internet).

7. *See generally* CROSS-INDUSTRY WORKING TEAM, *supra* note 6.

8. *See infra* text accompanying notes 207-29 for a discussion of whether XIWT's cybercash system is compatible with RFC 1422. Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, RFC 1422 (1993) (available from Internet Engineering Task Force). The Internet Engineering Task Force ("IETF") is a voluntary, cooperative body that discusses and formulates standards and protocols for the Internet through documents called Requests For Comments ("RFCs").

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 3 1996

electronic credit card systems, however, because measures intended to prevent counterfeiting and otherwise to authenticate the cybercash token make a cybercash transaction look very much like a credit card transaction. Thus, from the perspective of a purchaser or merchant, the technological and legal infrastructure required for a secure cybercash transaction may appear to be the same. The redemption obligation of the cybercash issuer, however, may differ from that of the credit card issuer. These differences vary according to the specificity of the fund used for redemption, the possibility of a stop-payment order in a credit card transaction, or the greater likelihood of defenses to redemption against those presenting credit card charges, based on federal law, compared with those presenting cybercash for redemption.[9]

Credit card and cybercash systems for the Internet must be supported by an appropriate technological and legal infrastructure. The infrastructure must address the two types of risk which would otherwise discourage use of any type of payment system: the risk of dishonor and the risk of forgery. The legal infrastructure responsible for the risk of dishonor must accomplish two things: first, it must ensure that one who accepts cybercash or a credit card has a legal claim against the issuer for redemption of the debt, and second, it must assure a fund from which redemption can be made.

The technological infrastructure for managing the risk of forgery must make it difficult or impracticable to forge the signature of an authorized signatory, and also must make it difficult or impossible to counterfeit the authorization of a bank or other issuer. For the

---

9. If cybercash is to remain distinct from credit cards, there must be some superior position for a holder in due course. A holder in due course may enforce the obligation of the issuer of commercial paper, such as a bill of exchange, despite defenses that might be available to the original owner of the paper. *See* U.C.C. § 1-201(20) (1995) (definition of "holder"); U.C.C. § 3-301 (rights of a "holder"); U.C.C. § 3-302 (definition of "holder in due course"); U.C.C. § 3-305 (rights of a holder in due course). The holder in due course doctrine increases the willingness of intermediaries to accept commercial paper because it increases the likelihood of redemption and decreases the possibility of dishonor. Private bank notes and most traveler's checks—the closest paper analogies for digital cash—qualify transferees for holder in due course status because they are "negotiable instruments." *See infra* text accompanying notes 37-72.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 4 1996

technological infrastructure to work as intended, a legal infrastructure must exist that defines the powers, rights, and privileges of participants in the technological infrastructure, especially certificate authorities.[10]

This article begins by reviewing the role that money and quasi-money such as traveler's checks, money orders, and credit card charges play in conventional payment systems, including the connection between banking regulation and these monetary issuances. The article then explains the commercial relationships in credit card and proposed cybercash systems on the Internet. The article ultimately argues for necessary changes in technological and legal infrastructures necessary to protect consumers and merchants from the risk of dishonor and the risk of forgery.

The immediate steps that should be taken are the enactment of more digital signature laws such as the one recently adopted by the Utah legislature; the encouragement of proliferation of the flourishing of certificate authorities; and the development of private technical and legal networks for settlements among consumers, merchants, merchant banks, and issuers. Consumer protections under existing legislation are adequate, therefore banking regulators should wait to determine if any significant problems develop with respect to dishonor of payment orders by issuers before intervening.

II. LEGAL POSITION OF CONVENTIONAL MONEY: ASSURING A RIGHT TO REDEMPTION

The definitive payment system is money. Money in circulation is classified as one of two types based on its value. The first type has value because it is legal tender.[11] The second type has value because it represents a debt of a trustworthy debtor.[12]

---

10. *See infra* text accompanying notes 212-17 for a further discussion of certificate authorities.

11. *See, e.g.*, The Legal Tender Cases, 79 U.S. (12 Wall.) 457 (1870) (upholding statutes making paper currency legal tender, along with gold and silver).

12. *See, e.g.*, The Gold Clause Cases, 294 U.S. 240, 362-64 (1935) (McReynolds, J., dissenting) (reviewing nature of gold certificates as solemn promises, and contrasting with nature of gold and silver).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 5 1996

Until relatively recently, most currency was issued by either state or nationally-chartered banks.[13] The common perception that only governments issue currency is misplaced. This section explores the legal position of various types of money in terms of the legal position of the holder vis-a-vis the issuer.

Early paper money systems suffered from redemption problems, especially when governments were issuers. In the colonial era, state-issued currency gained such a bad reputation that the Constitution prohibited its issue,[14] at least at the state level.[15]

---

13. The National Currency Act of 1863 authorized national banks to exercise powers including "obtaining and issuing circulating notes." Act of Feb. 25, 1863, ch. 58, § 11, 12 Stat. 665, 668 (1863). The 1863 Act was replaced by the National Banking Act of 1864 which prohibited banks from issuing "post notes or any other notes to circulate as money" other than the ordinary bank bills authorized by the Act. Act of June 3, 1864, ch. 102, § 23, 13 Stat. 99, 106 (1864) (codified as amended in scattered sections of 12 U.S.C. and 31 U.S.C.). *See generally* Howard H. Hackley, *Our Baffling Banking System*, 52 VA. L. REV. 565, 569-73 (1966) (reviewing history of American banking system). National banks which did not redeem their notes on demand by the note holders were subject to receivership imposed by the Comptroller of the Currency under section 50 of the National Banking Act of 1864, *supra*. *See, e.g.*, Cadle v. Baker, 87 U.S. 650, 651 (1874) (upholding receivership imposed on bank as against debtors of the bank). State bank notes were subsequently discouraged by the imposition of a 10% federal tax on their use by both state and federal banking associations. Act of March 3, 1865, ch. 78, § 6, 13 Stat. 469, 484; *see also* People v. Gould, 178 N.E. 133, 137 (Ill. 1931) (describing legislation imposing 10% tax on state bank notes).

14. U.S. CONST. art. I, § 10, cl. 1 ("No State shall . . . emit Bills of Credit").

15. *The Legal Tender Cases*, 79 U.S. (12 Wall.) at 546-47. Justice Bradley, in his concurrence, noted that when the Constitution was written, it had been the practice for most governments to employ the public credit as a means of "anticipating national revenues" to provide a medium of exchange "sometimes by the use of exchequer bills or bills of credit, and sometimes by pledges of the public domain." *Id.* at 556-57 (Bradley, J., concurring). Bills of credit were issued by colonial governments until Parliament prohibited the practice under pressure from English merchants. *See id.* (Bradley, J., concurring). The prohibition in New England began in 1751 and was extended to all the colonies in 1763. *See id.* (Bradley, J., concurring). While England had not made its exchequer bills legal tender, it had established the Bank of England which issued large numbers of circulating notes. *See id.* at 568 (Bradley, J., concurring). These notes could not by law be redeemed in specie so that England's gold and silver reserves could be used for foreign exchange instead of for currency purposes. *See id.* (Bradley, J., concurring). Thus, notes issued by the Bank of England became legal tender. *See id.* at 568-69 (Bradley, J., concurring). Much

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 6 1996

Typically, the evils associated with government-issued bills of credit "were the want of some real and substantial fund being provided for their payment and redemption, and no mode provided for enforcing the payment of the same."[16] While bills of credit issued by states were not enforceable because of sovereign immunity,[17] private issuances usually were supported by the general credit of the issuer,[18] which was reachable through common law actions for debt.

Paper money is a subclass of commercial paper. All bank bills and bank notes are bills of credit. A bill of credit is "negotiable paper, intending to pass as currency or as money, by delivery or endorsement."[19] The nature of bills of credit is not changed, whether the negotiable paper is issued by a corporation or by a state.[20] Bills of credit originally involved a variety of evidences of debt, including bank-issued notes intended to circulate as currency. In its mercantile sense, the term meant a letter addressed by one merchant to another to give credit to the bearer for money or goods, also known as a bill of exchange. The three crucial attributes of bills of exchange were (1) a contract to pay money at

---

more recently, the State of California issued "IOUs" to its employees in lieu of paychecks in response to a budget crisis. Paul Jacobs, *If It's a Crisis, How Come Nothing's Changed?*, L.A. TIMES, July 27, 1992, at A3. The employees experienced some difficulty in getting banks to accept the state IOUs and to credit their accounts. *Id.* Such IOUs functioned essentially as state-issued currency. *Id.*

16. Briscoe v. Bank of Ky., 36 U.S. (11 Pet.) 257, 327 (1837) (Thompson, J., concurring) (concurring in holding that banking entity financed by the State of Kentucky could issue bank notes without violating the Constitution's prohibition of state issuance of bills of credit).

17. *See id.* at 295.

18. *See id.* at 294-95 (plaintiff arguing that security of private bank notes rests on general credit of issuer).

19. *See id.* at 330 (Story, J., dissenting) (explaining bills of credit and banknotes and their relationship to money).

20. *See id.* at 331 (Story, J., dissenting). Justice Story agreed with the majority on the nature of money as commercial paper. *Id.* (Story, J., dissenting). He did not, however, think that the constitutional prohibition would extend to private bank issuances of bills, thus finding a way to invalidate the Bank of Kentucky without invalidating the principal means of currency. *Id.* at 348 (Story, J., dissenting) (arguing that no evils flowed from private issuance of bills, only from state issuances).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 7 1996

a future date, (2) payment resting on the security, faith, and credit of those who put the bill in circulation, and (3) legal enforceability.[21]

The Constitution itself prevented states from issuing money.[22] Private bank notes from state-incorporated banks had narrowly escaped prohibition in *Briscoe v. Bank of Kentucky*,[23] when the Supreme Court rejected a claim that Kentucky was prohibited by the Constitution from chartering a state bank which functioned like a private bank by issuing demand notes intended to circulate as currency.[24]

Federal law required the use of gold and silver in transactions with the national government and most states required bank notes to be redeemed on demand in coin.[25] From 1846, when the Independent Treasury Bill was passed,[26] until the Civil War, the federal government was kept separate from the banking system by making the government its own banker and by keeping government funds in the vaults of independent treasury office banks.[27]

To meet the needs of the Civil War, the national banking system was established. Congress authorized the issuance of "treasury notes" and subsequently made them legal tender. The final step in nationalizing the currency was to impose a ten percent tax on state bank notes and notes of any person used for circulation.[28] This ten percent surcharge was characterized seventy years later as

---

21. *Id.* at 328 (Baldwin, J., concurring).

22. *See supra* notes 14-15 and accompanying text.

23. 36 U.S. (11 Pet.) 257 (1837).

24. *Id.* The Supreme Court held that the establishment of a bank wholly owned by Kentucky, which had capital provided entirely by Kentucky, did not violate the constitutional prohibition against states emitting bills of credit. *Id.* at 327.

25. *See* Veazie Bank v. Fenno, 75 U.S. (8 Wall.) 533, 536-37 (1869) (discussing federal and state currency requirements).

26. Act of Aug. 6, 1846, ch. 90, 9 Stat. 59-66 (establishing the Treasury, the Secretary of the Treasury, a system of mints and depositions, and an administrative apparatus for management of "public money").

27. *See, e.g.*, Raichle v. Federal Reserve Bank, 34 F.2d 910, 912-14 (2d Cir. 1929) (providing a history of the federal government's regulation of the banking and monetary system).

28. *See Veazie Bank*, 75 U.S. (8 Wall.) at 538-39 (rejecting challenges to the tax which argued that it was an unconstitutional direct tax).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 8 1996

a prohibitive tax intended to protect the national currency from interference by issues of state bank notes.[29]

In the *Legal Tender Cases*,[30] the Court allowed Congress to establish federal currency as legal tender on a national basis.[31] Private bank notes, however, had never been legal tender.[32] Justice Bradley, in his concurrence in the *Legal Tender Cases*, endorsed the Court's conclusion that the national government had the power to issue currency and to make it legal tender because that power was prohibited to the states except through the charter of local banks which provide "inadequate, fluctuating, uncertain, and insecure" currencies.[33] Many states responded to the ten percent tax by prohibiting the organization of any more "issuing banks."[34] National banks were also subject to regulation, but by Congress rather than by the state.[35] As a result, by the turn of

---

29. *See* Campbell v. Chase Nat'l Bank, 5 F. Supp. 156, 168-69 (S.D.N.Y. 1933) (upholding legislation prohibiting private gold hoarding based on the need to protect the national currency system).

30. 79 U.S. (12 Wall.) 457, 465 (1870)

31. *See The Legal Tender Cases*, 79 U.S. (12 Wall.) at 465 (holding Congressional issuance of legal tender to be constitutional).

32. *See* Briscoe v. Bank of Ky., 36 U.S. (11 Pet.) 257 (1837) (holding that a state-chartered banking corporation does not retain the state's sovereign immunity).

33. *The Legal Tender Cases*, 79 U.S. (12 Wall.) at 562 (Bradley, J., concurring).

34. *See, e.g.*, People v. Gould, 178 N.E. 133, 137 (Ill. 1931) (reviewing statutory prohibition of state bank currency in applying statute which prohibits the acceptance of deposit by an insolvent bank); Seymour v. Greve, 81 N.W. 1059, 1060 (Minn. 1900) (taking judicial notice that no bank in Minnesota had issued bank notes since the imposition of the 10% federal tax, and concluding that the state legislature had removed such banking powers in 1895); State *ex rel.* Caples v. Hibernian Sav. & Loan Ass'n, 8 Or. 396, 399-401 (1880) (describing legislative history of Oregon state constitutional prohibition on chartering banks which issue currency); Luckey v. State, 26 Tex. 362 (1862) (affirming conviction of individual for issuing bills, but lacking discussion of the genesis of the prohibition).

35. *See, e.g.*, Cosmopolitan Trust Co. v. Mitchell, 136 N.E. 403, 406 (Mass. 1922) (discussing statutory authority of the Comptroller of Currency to seize property and assets of a nationally-chartered bank when it refuses to pay its circulating notes); Smith v. Exchange Bank, 26 Ohio St. 141 (1875) (determining that nationally-chartered banks are subject to Congressional usury legislation to which individuals are not).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 9 1996

the century the currency had been significantly nationalized.[36]

Nationalizing the currency had the effect of encouraging the invention of a variety of quasi-currencies, most significantly, personal checks and traveler's checks.[37] The ten percent tax simply shifted private money from bank notes to demand deposits and checks.[38] Historically, the traveler's check was a consolidation of a traveler's letter of credit and separate drafts drawn upon the authority created by the letter.[39] Because traveler's checks do not become bearer paper until they are countersigned in the presence of the acceptor, they are not cash equivalents until that time. Traveler's checks, however, are as reliable as cash. They also are safer for the purchaser than cash because of the issuer's promise to replace them if they are lost or stolen.[40]

As the private quasi-currencies matured, the nationalization of the currency continued. The next major legislative step was taken with the establishment of the Federal Reserve System.[41] The 1908 Aldrich-Vreeland Act[42] regulated the issuance of emergency currency by banks on shaky financial footing.[43] The Federal Reserve Act[44] followed as a response to the bank panic of 1907.[45] Among other things, the Federal Reserve Act intended

---

36. *See, e.g.*, 9 C.J.S. *Banking* § 185 n.8 (1938) (explaining that since most states have statutes prohibiting banks from issuing money instruments, that function is exercised only by national and federal reserve banks).

37. *See generally* 42 BANKING L.J. i-xxx (1925) (table of contents) (containing numerous articles and digest entries on personal checks and traveler's checks, but no articles on circulating currency).

38. JOHN J. GALBRAITH, MONEY: ONCE IT CAME, WHERE IT WENT 90 (Houghton Mifflin 1975).

39. Note, *Negotiability of Traveler's Checks*, 47 YALE L.J. 470, 472 (1938).

40. Xanthopoulos v. Thomas Cook, Inc., 629 F. Supp. 164, 173-74 (S.D.N.Y. 1985) (explaining deferred conversion into cash equivalents).

41. *See* Raichle v. Federal Reserve Bank, 34 F.2d 910, 912 (2d Cir. 1929) (citing 12 U.S.C. §§ 221-522).

42. Pub. L. 60-169, 35 Stat. 546 (1908) (codified as amended at 12 U.S.C. § 104 (1994)).

43. *See, e.g.*, John A. Deangelis, Note, *Riches Do Not Last Forever: Real Estate Investment By National Banks*, 1991 U. ILL. L. REV. 777, 785 n.85.

44. Pub. L. 63-43, 38 Stat. 251 (1913) (codified as amended at 12 U.S.C. § 221 *et. seq.* (1994)).

45. *Id.* at 785.

to abolish the existing bond-secured note issue.[46] National banks were required to belong to the system and were encouraged to surrender the bonds that secured their own note issues, although this did not become a requirement until 1935.[47] Still, sixty-five percent of all banks remained outside the system as late as 1929.[48] By the Depression, most of the currency consisted of gold and silver certificates issued by Federal Reserve Banks and the Treasury.[49]

The Banking Act of 1933[50] established the Federal Deposit Insurance Corporation, and required all federal reserve system banks, state and federal, to participate in its deposit insurance program,[51] though it did not explicitly address bank notes as currency.[52] The Gold Repeal Joint Resolution[53] eliminated private contractual obligations that payment be tendered in gold,[54] and thus effectively disconnected paper currency from the gold standard.[55] In any event, by 1938, one court characterized notes

---

46. *Id.* at 813.

47. GALBRAITH, *supra* note 38, at 124-25.

48. *Id.* at 127.

49. *See* Norman v. Baltimore & O.R.R., 294 U.S. 240, 316 & n.1 (1935) (McReynolds, J., dissenting) (reviewing nature and quantity of gold certificates).

50. Act of June 16, 1933, Pub. L. No. 66, ch. 89, 48 Stat. 162, 162 (1933) (codified at 12 U.S.C. § 227 *et. seq.* (1994)).

51. 48 Stat. at 169.

52. *But see* Banking Act of 1933 § 16, 48 Stat. at 184, amending R.S. 5136 p. 993, 12 U.S.C. § 24 (Supp. VI 1932) (authorizing national banking associations to issue circulating notes). National banking associations are synonymous with national banks. 18 U.S.C. § 656 historical note (terms synonymous under definitions of 12 U.S.C. § 12 (1940)).

53. Ch. 48, 48 Stat. 113 (1933) (codified at 31 U.S.C. § 5118(d)(2) (1994)).

54. Such clauses encouraged the hoarding of gold which diminished the quantity available to serve as reserves for paper currency and made it impractical to increase the quantity of paper currency beyond the supply of gold to serve as a redemption standard. *Norman*, 294 U.S. at 296 (explaining the problem of justifying invalidation of private gold clauses); Holyoke Water Power Co. v. American Writing Paper Co., 83 F.2d 398 (1st Cir. 1936) (voiding contractual provision requiring payment in gold), *aff'd*, 300 U.S. 324 (1937); Campbell v. Chase Nat'l Bank, 5 F. Supp. 156, 168 (S.D.N.Y. 1933) (same), *aff'd*, 71 F.2d 669 (2d Cir.), *appeal dismissed*, 291 U.S. 686 (1934).

55. Norman v. Baltimore & O.R.R., 294 U.S. 240, 311 (1935) (upholding constitutionality of legislation voiding clauses contained in virtually all private contracts requiring payment in gold).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 11 1996

issued by Federal Reserve banks as the predominant form of circulating currency.[56] An order issued in November 1967 suspended silver sales from the Treasury's stock and directed the Treasury to retire silver certificates and replace them with Federal Reserve notes.[57]

Today's private bank note is the traveler's check, instead of the bank note, because customers insist on replacement, thereby losing little in liquidity when using traveler's checks.[58] Customers may, however, lose some anonymity because a record of traveler's check purchases is kept. A cybercash token is analogous to a money order or traveler's check as much as to currency.[59]

Little case law exists on the legal characteristics of traveler's checks and one New York trial court characterized them as "somewhat of a legal anomaly."[60] Traveler's checks can be

---

56. Geery v. Minnesota Tax Comm'n, 278 N.W. 594, 598 (Minn. 1938) (stating that the major share of currency in circulation is "in the form of Federal Reserve Bank Notes which are obligations of the United States and the quantity of which is within the control of the Federal Reserve Board").

57. *Redemption of Silver Certificates: Hearing on H.R. 7476 Before the Comm. on Banking and Currency of the House of Representatives*, 90th Cong., 1st Sess. 12 (1967) (statement of Joseph W. Barr, Under Secretary of the Treasury).

58. The main difference between instruments like traveler's checks and bank officer checks versus personal checks is that a personal check is the obligation of the drawer only until the drawer bank accepts it, while traveler's checks and bank officer checks are the obligation of the issuer as soon as they become negotiable. *See generally* U.C.C. § 3-122 (1995) (describing the accrual of cause of action against makers and acceptors); U.C.C. § 3-410 (stating how an acceptor may vary a draft).

59. A cybercash token is unlike a personal check because it represents a legal obligation of the issuer when it is used for a purchase, whereas a personal check does not become the legal obligation of the drawee bank until it is "accepted" by the bank at the end of the negotiation process.

60. First Nat'l City Bank v. ABC, 328 N.Y.S.2d 326, 329 (Sup. Ct. 1971) (finding that a bank which issued traveler's checks was entitled to recover from a selling agent for negligence in losing several blank checks which were presented and paid before the issuing bank learned of the loss or larceny); *see also* Ashford v. Thomas Cook & Son, 471 P.2d 530, 533 & nn.2-3 (Haw. 1970) (finding that traveler's checks do not fall entirely within the purview of Negotiable Instruments Law, but the public's acceptance of them as a medium of exchange means they have acquired negotiable characteristics; accordingly the issuer of traveler's checks bore all risks of theft and was obligated to pay the bona fide holder in due course who paid valuable consideration).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 12 1996

issued both by banks, such as CitiCorp, or by non-banks such as American Express or Thomas Cook.[61] Bank traveler's checks are legally identical to other kinds of officers' checks, including cashier's checks, money orders, bank drafts, certified checks, and certificates of deposit. In substance, they are all promissory notes of the bank and are negotiable instruments.[62] When a traveler's check is issued by a non-bank, the traveler's check still is a negotiable instrument,[63] but the maker is an entity other than a bank, and thus the obligation to pay is that of the non-bank.[64] U.C.C. section 3-104 establishes the following requirements and definitions for negotiable instruments:

> (1) Any writing to be a negotiable instrument within this Article must
>
> > (a) be signed by the maker or drawer; and
> > (b) contain an unconditional promise or order to pay a sum certain in money and no other promise, order, obligation or power given by the maker or drawer except as authorized by this Article; and
> > (c) be payable on demand or at a definite time; and
> > (d) be payable to order and to bearer.

---

61. *See* Sony Corp. of Am. v. American Express Co., 455 N.Y.S.2d 227, 229 (Civ. Ct. 1982) (distinguishing between bank money orders and money orders issued by American Express, and determining that the bank was the only sales agent of American Express).

62. Bank of Am. Nat'l Trust & Sav. Ass'n v. Cranston, 60 Cal. Rptr. 336, 341-42 (App. Ct. 1967) (finding that the Uniform Disposition of Unclaimed Property Act covered bank drafts, cashier's checks, certified checks, money orders, and Christmas Club checks).

63. Xanthopoulos v. Thomas Cook, Inc., 629 F. Supp. 164, 171-72 (S.D.N.Y. 1985) ("identifying signature that makes traveler's checks negotiable instruments is not the counter signature but the signature made when checks are first purchased by the issuer"); Thomas C. Cook, Inc. v. Rowhanian, 774 S.W.2d 679, 682 (Tex. Ct. App. 1989) (stating that traveler's check containing a purchaser's first identifying signature is a negotiable instrument and that a purchaser's counter signature converts check to a bearer paper that is negotiable by delivery alone); U.C.C. § 3-104 cmt. 4 (amended 1990) ("Traveler's checks in the usual form, for instance, are negotiable instruments under this Article when they have been completed by the identifying signature").

64. *Sony Corp. of Am.*, 455 N.Y.S.2d at 229. When traveler's checks are issued by non-banks, they typically are made payable through a bank that performs clearing and paying functions by a prior arrangement with the issuer. *Id.*

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 13 1996

> (2) A writing which complies with the requirements of this section is
>
> > (a) a "draft" ("bill of exchange") if it is an order;
> > (b) a "check" if it is a draft drawn on a bank and payable on demand;
> > (c) a "certificate of deposit" if it is an acknowledgment by a bank of receipt of money with an engagement to repay it;
> > (d) a "note" if it is a promise other than a certificate of deposit.[65]

The maker of a traveler's check is the issuer. The purchaser gives the issuer cash, and the issuer gives the purchaser a note for that amount in the form of a traveler's check. The note is payable to the order of the purchaser and is payable on demand, thus satisfying the second and third requirements of negotiable instruments. The note also contains an unconditional promise or order to pay a sum in certain money with no other promise, order, obligation, or power.[66] The consideration for traveler's checks, and thus the inducement for issuers, is the use of the purchaser's money until the traveler's checks are presented for redemption—the "float."[67] One could argue that traveler's checks do not qualify as negotiable instruments under the literal requirements of Article III, because they are conditional upon counter-signature, thereby failing U.C.C. section 3-104(1)(b). Also, some traveler's check forms state that they are to be paid only out of a particular fund or source, thus making them conditional under U.C.C. section 3-105(2)(b). Despite these characteristics, traveler's checks have been treated for more than one hundred years as negotiable instruments.[68] Section 1-205 of the U.C.C. expressly

---

65. U.C.C. § 3-104 (1995).

66. *Xanthopoulos*, 629 F. Supp. at 172 (matching the characteristics of traveler's checks with the requirements of U.C.C. § 3-104(1) and denying payment on traveler's checks which were not countersigned in the presence of the acceptor).

67. *See id.* at 171 n.7; *Thomas C. Cook*, 774 S.W.2d at 681-82 (characterizing consideration). Most traveler's check issuers also charge a fee to the person buying the traveler's checks. *Id.*

68. *See* E. P. Ellinger, *Travellers' Cheques and the Law*, 19 U. TORONTO L.J. 132, 139 & n.22 (1969) (explaining why traveler's checks do not literally

authorizes usage of trade as a means of interpreting the U.C.C.,[69] and 100 years of interpretation surely qualifies as usage of trade.

Negotiable instruments improve the position of a holder in due course vis-a-vis the issuer.[70] Negotiability thus enhances the crucial attributes of currency identified by the Supreme Court over a century ago.[71] Therefore, a cybercash token that constitutes a negotiable instrument is preferable to a token that is not negotiable. In order to be a negotiable instrument, the token must be in "writing" and must be "signed" by the maker. Thus, electronic messages used in payment systems must meet the writing and signature requirements.[72]

III. DEFINITION OF BANKING FUNCTION

The legal history of money is inseparable from the legal history of banking. A contract claim against an issuer of money is worth little if the assets of the issuer are insufficient to cover redemption. Understanding the interrelationship of money and banking regulation is helpful in determining whether issuance of cybercash is permissible only within the framework of banking regulation, or whether some other form of assurance of a fund for redemption of cybercash and credit card obligations is also a possibility. Although at common law anyone could engage in the business of banking, corporations could exercise only those powers granted in their charters, and virtually no general corporation law permits a

---

qualify under the U.C.C. and why usage justifies treating them as negotiable instruments).

69. U.C.C. § 1-205. Moreover, the comment to U.C.C. section 3-104(i) expressly states that traveler's checks are negotiable instruments. *See supra* note 63.

70. *See Xanthopoulos*, 629 F. Supp. at 172 (indicating that a holder in due course is not subject to the defenses that an issuer might have against a holder not in due course); U.C.C. § 3-305 (rights of holder in due course).

71. *See supra* note 21 and accompanying text.

72. *See* MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW ch. 6 (1991) (discussing ways in which electronic messages satisfy statutes of frauds and other signature and writing requirements).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 15 1996

non-banking corporation to engage in banking.[73] Chartering of bank corporations long has been integrated with banking regulation.

The preceding discussion explained that at the beginning of the Civil War, circulating currency consisted almost entirely of bank notes issued by private banks incorporated under state law.[74] Because their redeemability was not certain, bank notes circulated at a discount.[75] States were prohibited by the Constitution from issuing notes as money,[76] and until the *Legal Tender Cases*,[77] it was questionable whether Congress had such power.[78] Thus, the only way state or federal law could protect against the risk of dishonor[79] was to set requirements for incorporation of national or state banks. For example, enterprises wishing to engage in the business of banking had to meet paid-in capital requirements and could issue only a certain percentage of capital in notes.[80] A certain amount of specie had to be kept on hand to redeem outstanding notes. Some of these requirements were expressed directly in banking statutes,[81] while others were expressed in the charters of banking corporations.[82]

As in any regulatory regime, the regulation of banking required a definition of the activity to be regulated.[83] Questions arose

---

73. 9 C.J.S. *Banks and Banking* § 4 (1938) (characterizing a corporation's power to transact banking business as dependent on the state's grant of corporate powers).

74. *See* Veazie Bank v. Fenno, 75 U.S. (8 Wall.) 533, 536 (1869).

75. James A. Dietz, *Personal Policy and Judicial Reasoning: Salmon P. Chase and* Hepburn v. Griswold, 21 N. KY. L. REV. 235, 238-39 (1993).

76. Houston & Tex. Cent. R.R. v. Texas, 177 U.S. 66, 85 (1900).

77. *See* The Legal Tender Cases, 79 U.S. (12 Wall.) 457 (1870).

78. *Id.* at 467.

79. Dishonor results from an inability or unwillingness of an issuer of a payment obligation to redeem it. For a further discussion on the risk of dishonor, *see infra* part V.B.

80. Veazie Bank v. Fenno, 75 U.S. (8 Wall.) 533, 539 (1869).

81. *See e.g.*, Provident Inst. v. Massachusetts, 73 U.S. (6 Wall.) 611 (1867).

82. *See e.g.*, Farrington v. Tennessee, 79 U.S. 679 (1877); State v. Stoll, 84 U.S. (17 Wall.) 425 (1873); Furman v. Nichol, 75 U.S. (8 Wall.) 44 (1868).

83. One commentator defined "bank" as:

> an institution, usually incorporated, with power to issue its promissory notes, intended to circulate as money (known as 'bank notes'), or to receive the money of others on general deposit, to form a joint fund

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 16 1996

about certain instruments like cashier's checks or certified checks that, according to the Supreme Court, circulated as money or at least as currency. In 1899, the Supreme Court stated:

> The very first banking in England was pure borrowing. It consisted in receiving money in exchange for which promissory notes were given payable to bearer on demand, and so essentially was this banking as then understood, that the monopoly given to the Bank of England was secured by prohibiting any partnership of more than six persons "to borrow, owe or take up any sum or sums of money on their bills or notes payable at demand." And it had effect until 1772, (about thirty years,) when the monopoly was evaded by the introduction of the deposit system. The relations created are the same as those created by the issue of notes. In both a debt is created - the evidence only is different. In one case it is a credit on the banker's books; in the other his written promise to pay. In the one case he discharges it by paying the orders (cheques) of his creditor; in the other, by redeeming his promises. These are the only differences. There may be others of advantage and ultimate effect, but with them we are not concerned.[84]

The core functions of the business of banking are the acceptance

---

> that shall be used by the institution for its own benefit, for one or more of the purposes of making temporary loans and discounts, of dealing in foreign and domestic bills of exchange, coin, bullion, credits, and the remission of money, or with both these powers, and with privileges in addition to these basic powers of receiving deposits and making collections for the holders of negotiable paper if the institution sees fit to engage in such business.

State v. Comptoir Nat'l D'Escompte de Paris, 26 So. 91, 96 (La. 1899) (quoting 1 MORSE, BANKS § 2).

Another commentator stated that "[a] banker is a trader who buys money, or money and debts" by creating other debts, which he does his exchanging a debt payable in the future for one payable on demand. HENRY D. MACLEOD, THE THEORY AND PRACTICE OF BANKING 110 (2d ed. 1866). This, Macleod says, is the essential definition of "banking." *Id.* "The first business of a banker is not to lend money to others, but to collect money from others." *Id.*

James W. Gilbart defines a banker, however, to be "a dealer in capital, or, more properly, a dealer in money." 1 JAMES W. GILBERT, THE ELEMENTS OF BANKING: WITH TEN MINUTES' ADVICE ABOUT KEEPING A BANKER 2 (2d ed. 1854). A banker is an intermediate party between the borrower and the lender who "borrows of one party and lends to another." *Id.*

84. Auten v. United States Nat'l Bank, 174 U.S. 125, 142 (1899).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 17 1996

of deposits and the making of loans.[85] Other traditional definitions are circular, and therefore, not very helpful. One dictionary, for instance, has defined "deposit" in banking law as "[t]he act of placing money in the custody of a bank or banker, for safety or convenience, to be withdrawn at the will of the depositor or under rules and regulations agreed on."[86] Except for the state prohibitions on issuing currency, noted above, most definitions contemplate issuance of circulating currency as falling within the banking function.[87]

Nevertheless, the issuance of traveler's checks and money orders or other commercial paper, irrespective of their negotiability, does not necessarily constitute banking. The limited case law assumes that a variety of currency equivalents, such as money orders and traveler's checks, can be issued by private money lenders.[88] Accordingly, there is no reason to conclude that issuance of cybercash resembling traveler's checks or money orders in legally pertinent detail will subject the issuer to banking regulation. It follows that cybercash is simply a private negotiable "paper."[89]

---

85. Staunton Indus. Loan Corp. v. Commissioner, 120 F.2d 930, 933-34 (4th Cir. 1941) (stating that the chief functions are receipt of deposits from general public, issue of deposit funds for secured loans, and relationship of debtor and creditor between bank and depositor; finding industrial loan corporation under state statute entitled to federal tax exemption reserved for banks because corporation accepted "certificates of investment" on demand for withdrawal of deposits and also honored them if negotiated).

86. BLACK'S LAW DICTIONARY 438 (6th ed. 1990).

87. 9 C.J.S. *Banks & Banking* § 1(c) (1938) (banking includes "issuing notes payable on demand and intended to circulate as money").

88. A private money lender is not necessarily a bank. State v. Comptoir Nat'l D'Escompte de Paris, 26 So. 91, 95-96 (La. 1899) (citing Seldon v. Trust, 94 U.S. 419 (1876)) (construing a state statute regarding bank licensing requirement to exclude foreign corporations that issued bills of credit for receipt of cotton, redeemable in France and finding that such conduct did not fall within traditional definition of banking). Some early cases distinguish, without persuasive analysis, the sale of money orders from banking. *E.g.*, Wells, Fargo & Co. v. Northern Pac. R.R., 23 F. 469, 471-72 (D. Or. 1884) (concluding that the selling of telegraphic money orders was not the business of banking; rather the bank was merely transporting the money).

89. *See generally* Ellinger, *supra* note 65; William D. Hawkland, *American Traveler's Checks*, 15 BUFF. L. REV. 501 (1965-66) (preferring to treat traveler's checks as negotiable instruments because industry practices and public expectations favor such treatment); Note, *Negotiability of Traveler's Checks*, 47 YALE

It is also plausible, however, to conclude that the money paid to the issuer of cybercash, like the money paid to the issuer of traveler's checks, constitutes a "deposit."[90] Because acceptance of deposit is one of the two traditional hallmarks of the business of banking, this characterization may lead to cybercash issuers being classified as banks.

If banking regulation does not cover the full range of issuances of money or quasi-money—as it obviously does not when one considers American Express traveler's checks, Seven-Eleven money orders, and non-bank credit cards—how else does the legal system assure availability of a fund for redemption? The principal answer is that the legal system relies on the market, backed up by contract law. American Express traveler's checks are accepted because the market trusts that American Express will remain solvent. Money orders from Seven-Eleven are accepted because people believe that Southland Corporation will have funds available to redeem them.[91] In other words, payment systems do not always look to the law to assure a fund for redemption; some systems are satisfied by the existence of a legal right against the issuer.

L.J. 470 (1937-38) (noting that traveler's checks have acquired negotiability through custom and not through the provisions of the Negotiable Instruments Law); Note, *Personal Money Orders and Teller's Checks: Mavericks Under the U.C.C.*, 67 COLUM. L. REV. 524 (1967) (arguing that courts should fulfill a typical purchaser's expectations and permit stop payment on traveler's check); J.A. Bryant, Jr., Annotation, *Rights of One Who Acquires Lost or Stolen Traveler's Checks*, 42 A.L.R.3d 846 (1972) (noting application of Uniform Negotiable Instruments Act to traveler's checks in most cases).

90. In Bank of America Nat'l Trust & Savings Ass'n v. Cranston, 60 Cal. Rptr. 336 (Ct. App. 1967), the California Intermediate Appellate Court treated money paid for bank drafts, cashier's checks, certified checks, money orders, and Christmas Club checks as well as outstanding traveler's checks as deposits, under the guidance of Federal Reserve definitions, for purposes of state Unclaimed Property Act. *Id.* at 342 (citing 12 C.F.R. § 204.1(f) (1963)). Characterization of such instruments and deposits for this statutory purpose does not, of course, mean that they should be so characterized for purposes of defining the scope of banking regulation. *Id.*

91. This confidence may be misplaced. For instance, Southland Corporation, the owner of several Seven-Eleven stores, declared bankruptcy in the early 1990s. *See In re* Southland Corp., 124 B.R. 211 (Bankr. N.D. Tex. 1991) (rejecting the reorganization plan).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 19 1996

IV. BASIC CREDIT CARD RELATIONSHIPS

Much existing payment law pertinent to the National Information Infrastructure (NII) is private law: a web of contracts usually derived from a master contract language written by banking and credit card associations. The following sections explain the evolution of credit cards, work through the basic bilateral relationships involved in modern credit card transactions, and explain how these fit into a framework defined by major credit card associations such as VISA and MasterCard.

A. *Credit Card Transactions Rival Currency, Checks, and Money Orders as Payment Methods*

In 1938, the Philadelphia department store Wanamaker's unveiled the first credit system whereby customers could make payments by installment, rather than paying the full amount at the end of the billing period.[92] This "bipartite" system[93] included the customer/cardholder ("CH") and the merchant, who issued the cards for use in his store.[94] A subsequent and more complex version of the payment-by-installment credit system is the "tripartite" system.[95] Under the tripartite system, banks[96] issue credit

---

92. *See* Harvey L. Handley, III, Note, *Regulation of Revolving Credit Service Charges*, 28 WASH. & LEE L. REV. 386, 387 (1971) (noting the strong trend towards regulation of service charges accompanying the growth of revolving charge accounts). Before Wanamaker's began their free service, credit cards or credit coins permitted the customer to make purchases without paying cash, but required the customer to remit the full amount due at the end of the monthly credit period. *Id.* at 386-87.

93. The payment by installment procedure of credit is generally divided into two schemes. The bipartite system is made up of the customer/cardholder and the merchant who issues a card to the cardholder for use in the merchant's store. *Id.* at 387-88. The tripartite system is the more recent and complex system, and includes such common names as VISA, MasterCard, Diner's Club, and Discover Card. *See id.* at 388.

94. *Id.* Merchants who employ the bipartite system include large department stores and gasoline companies. *Id.* at 388 & n.18.

95. *Id.* at 388. The tripartite system began humbly in 1951 with local banks, and did not become national and profitable until the mid-1960s. *Id.*

96. Banks are no longer the only card issuing member of the tripartite system. Major corporations such as General Motors, Ford, Chrysler, and AT&T

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 20 1996

cards[97] to individuals who use them to purchase goods or services on credit from merchants who participate in the system and who are ultimately reimbursed by the issuing bank.[98] The three major entities which make up the system are held together by three separate written agreements.[99]

The relationship between the bank issuing the credit card and the merchant is usually not direct.[100] Most situations involve a merchant ("M") in an arrangement with his or her bank (merchant bank or "MB"), which in turn has an agreement with the issuing bank ("IB").[101] A written agreement between the merchant and

---

also issue credit cards which are operated essentially the same as bank credit cards. *See, e.g.*, *Credit Card for Chrysler*, N.Y. TIMES, Apr. 13, 1994, at D16. For convenience, this discussion will refer to all credit card issuing entities as banks. *See* Michael Duint, *Market Place*, N.Y. TIMES, Nov. 12, 1993, at D6.

97. Credit cards are defined by 15 U.S.C. § 1602(k) (1994) as "any card, plate, coupon book or other credit device existing for the purpose of obtaining money, property, labor, or services on credit."

98. Handley, *supra* note 92, at 388.

99. *See* National Bank of Can. v. Interbank Card Ass'n, 507 F. Supp. 1113, 1117-18 (S.D.N.Y. 1980) (describing tripartite arrangement consisting of agreements between bank and cardholder, bank and merchant, and cardholder and merchant). In addition to the customer/cardholder, the issuing bank, and the merchant, the tripartite system usually includes a merchant bank and "clearing-houses." Peterson v. Wells Fargo Bank, 556 F. Supp. 1100, 1109 n.16 (N.D. Cal. 1981). The merchant bank accepts deposits of credit slips from the merchant and forwards them to the issuing bank for credit of payment. *National Bank of Can.*, 507 F. Supp. at 1117. The clearinghouses provide billing, credit line authorization, reporting, and other related services to merchants and banks. *Id.* at 1118. "Both issuance to cardholders and signing of merchants occur within the framework of a bank credit card association to which a number of banks belong in an effort to market a single card . . . ." BARKLEY CLARK & BARBARA CLARK, THE LAW OF BANK DEPOSITS, COLLECTIONS AND CREDIT CARDS, ¶ 15.02[3] (4th ed. 1995).

100. Moreover, an issuing bank is prohibited from "requir[ing] a [merchant], as a condition to participating in a credit card plan, to open an account with or procure any other service from the [issuing bank] or its subsidiary or agent." 15 U.S.C. § 1666g (1994).

101. *See generally Peterson*, 556 F. Supp. at 1109 & n.16 (noting that merchants wishing to participate in a credit card program must enter into agreements with a bank which is a member of the program); *National Bank of Can.*, 507 F. Supp. at 1117-18 (discussing the contractual relationships involved in credit card plans); CLARK & CLARK, *supra* note 99, ¶ 15.02[4]. The relationship between the issuing bank and the merchant can be direct if the merchant's bank is the issuing bank of the card used by the customer.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 21 1996

the merchant bank regulates their relationship. The merchant bank coordinates the merchant's participation in the credit card system, collecting receipts from the merchant and transferring them to the issuing bank for credit on its own account at that bank.[102]

The terms of the merchant-merchant bank agreement are centered on the merchant's duty to honor a credit card for the purchase of his goods or services and the merchant bank's duty to accept the credit slip ("record of charge" or "ROC") from the merchant as a valid form of deposit.[103] The merchant may not discriminate against customers on the basis of which bank issued their credit card.[104]

The merchant must certify that the ROC was signed by the cardholder, that the ROC evinces an actual sale to the cardholder, and an "unconditional obligation" on the cardholder to satisfy the debt is represented by the ROC.[105] When the purchase price exceeds the maximum limit set by the agreement, the merchant must obtain authorization before completing the transaction.[106] The agreement may also contain provisions regulating the circumstances for which the merchant may accept the credit card. For example, the merchant may be proscribed from accepting the card for use on a down payment where the remainder is paid at another point, or from dividing a transaction into multiple sales in order to circumvent the limit.[107] The agreement may also prohibit the merchant from adding an extra charge to purchases made by credit card as opposed to cash or checks.[108]

The merchant bank must accept deposit of the credit slip and credit the merchant's account, less the agreed upon price, or

---

102. *National Bank of Can.*, 507 F. Supp. at 1117.
103. CLARK & CLARK, *supra* note 99, ¶¶ 15.02[4][b][i](1),(3).
104. *Id.* ¶ 15.02[4][b][i](6).
105. *Id.* ¶ 15.02[4][b][i](5).
106. *Id.* ¶ 15.02[4][b][i](7). Clearinghouses provide the service of authorizing permissible credit for individual cardholders. *See National Bank of Can.*, 507 F. Supp. at 1118.
107. CLARK & CLARK, *supra* note 99, ¶ 15.02[4][b][i](8).
108. *Id.* ¶ 15.02[4][b][i](2). Until 1984, when Congress allowed the provision to expire, federal law (formerly 15 U.S.C. § 1666f(a)(2)) statutorily prohibited this adding-on practice. *Id.* ¶ 15.02[4][b][i](2), n.18.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 22 1996

"discount rate" which the merchant bank charges for this service.[109] However, federal law prohibits the merchant bank from restricting the merchant from offering incentives or discounts for purchases made without the use of a credit card.[110]

Debit cards theoretically differ from credit cards in that they result in the issuing bank charging the card holder's deposit with the issuing bank rather than the issuing bank extending credit to the card holder. Many debit cards, however, can be financed by a line of credit and thus the two types of cards converge in practice. Merchants usually get a better rate on debit cards and consequently often prefer them.[111]

As the introduction noted, even cybermoney systems may resemble credit card systems in the their legal relationships. There are five entities or individuals in credit card transactions that are exposed to, or create, risk: the card holder ("CH"); the merchant ("M") who delivers goods and services in exchange for presentation of the credit card number and appropriate additional information; the unauthorized user ("U") who wants to obtain goods or services without paying for them, the issuing bank ("IB"), with whom CH has a contract; and the merchant bank ("MB"), with whom the merchant has a contract.

In the typical, legitimate (and non-Internet) credit card transaction, CH offers to buy merchandise or services from M, and gives M her credit card or credit card number. M contacts either IB or

---

109. *See id.* ¶¶ 15.02[4][b][i](1),(3).

110. *Id.* ¶ 15.02[4][b][i](2). 15 U.S.C. § 1666f(a) states that the issuing bank "may not, by contract, or otherwise, prohibit any such seller from offering a discount to a cardholder to induce the cardholder to pay by cash, check, or similar means rather than use a credit card." 15 U.S.C. § 1666f(a) (1994).

111. Debit cards are similar to credit cards in that charges made with them are paid out of an account specifically identified with the card holder. CLARK & CLARK, *supra* note 99, ¶ 16.05[1]. In this regard they are like personal checks and unlike bank checks and currency because a debit card is paid out of a fund contributed by the card holder in advance. *Id.* This represents a debt of the bank or other card issuer, while a credit card charge is paid after the fact by the card holder and after the charge is paid by the bank, but before the bank is reimbursed by the card holder, which represents an asset of the bank or other card issuer. *Id.*

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 23 1996

MB,[112] and communicates the credit card number, the amount of the transaction, and any other information required by the authentication procedure spelled out in the contract between M and MB. If the credit card number is valid for the amount of the transaction, M receives an authorization code. M delivers the merchandise or performs the service, and presents the record of charge—perhaps just the credit card number, the amount of the transaction, and the authorization code—to MB, and is paid immediately under the contract between M and MB. MB has a contract with IB that entitles MB to be paid in exchange for the ROC.[113] IB, in turn, is entitled to be paid by CH upon submitting a statement including the ROC.

B. *Sources of Credit Card Obligation*

Under the tripartite credit card system, banks issue credit cards to individuals who use them to purchase goods or services on credit from merchants participating in the system.[114] The merchants are reimbursed ultimately by the issuing bank.[115] The four major entities which make up the system, the cardholder, the merchant, the merchant's bank, and the issuing bank, are held together by three separate written agreements.[116] The whole system is tied together by a private network of clearance and settlement arrangements, and model contract language expressed in VISA and MasterCard bylaws and operating manuals.

As explained in the preceding section, the relationship between

---

112. Typically, MB provides the necessary hardware and software to enable M to obtain authorization through a network associated with the particular credit card.

113. This contract usually is found in the bylaws of the credit card venture, such as the VISA association. *See generally In re* Brendle's Stores, Inc., 165 B.R. 811, 814 (Bankr. M.D.N.C. 1993) (describing the typical contractual relationship).

114. *See* Handley, *supra* note 92, at 388.

115. *See id.*

116. *See supra* note 99 and accompanying text; *see also* Citizens & S. Nat'l Bank v. Thomas B. Hamilton Co., 969 F.2d 1013, 1014-15 (11th Cir. 1992); Broadway Nat'l Bank v. Progressive Casualty Ins. Co., 775 F. Supp. 123, 124-25 (S.D.N.Y. 1991). The clearinghouses provide billing, credit line authorization, reporting, and other related services to merchants and banks. *Citizens,* 969 F.2d at 1018.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 24 1996

the bank issuing the credit card and the merchant is usually not direct.[117] Most situations involve a merchant in an arrangement with its own bank (the merchant bank), which in turn has an agreement with a bank that is a member of the "network of financial institutions that processes . . . credit card transactions."[118] A written agreement between the merchant and the merchant bank governs the relationship between those two parties.[119] The merchant bank, in order to participate in the tripartite enterprise of credit card transactions and to acquire access to the network, enters into a separate agreement with a member entity of the credit card transaction network,[120] which can be an issuing bank.[121] As a result of this agreement, the merchant bank acquires access to the network through the issuing bank.

Broadway National Bank v. Progressive Casualty Insurance Co. exemplifies the relationship between a merchant bank and an issuing bank.[122] Broadway National Bank ("Broadway"), the merchant bank, entered into an "Associate Agreement" with Chemical Bank ("Chemical"), the issuing bank, which was a member of MasterCard International Incorporated.[123] The contract between Broadway and Chemical included a document setting forth the procedure for processing credit card transactions

---

117. *See supra* note 99 and accompanying text.

118. *Broadway Nat'l Bank*, 775 F. Supp. at 124; *see also supra* note 102 and accompanying text.

119. For a discussion regarding the agreement between the merchant and the merchant bank, see *supra* notes 101-10 and accompanying text.

120. The "network of financial institutions that processes MasterCard and VISA credit card transactions" is called "MasterCard International Incorporated." *Broadway Nat'l Bank*, 775 F. Supp. at 124.

121. *Id.*

122. *Id.*

123. *Id.* As a member bank, Chemical issued credit cards, served as a clearinghouse for credit card transactions, and brought local banks into the system. *Id.* Broadway was one of the local banks that contracted with Chemical. *Id.* It had agreements with merchants whereby it would accept deposits of credit sales slips and would credit the merchants' accounts for the purchase amounts. *Id.* For a discussion of the various terms contained in a merchant/merchant bank agreement, see *supra* notes 101-10 and accompanying text.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 25 1996

through the system.[124] As a result of a valid credit card transaction within this particular system, Broadway would be credited on its account with Chemical by Chemical, and Chemical would eventually be reimbursed by remittance from the cardholder for the amount billed by Chemical in a periodic statement.[125]

Questions of liability may arise in the context of a charge contested by the cardholder as a billing error made by the issuing bank.[126] A cardholder has sixty days from the date of the issuing bank's transmission of his statement to give the issuing bank written notice of a contested charge.[127] This notice triggers the "charge back" process.[128] The issuing bank investigates the validity of the cardholder's contention; if the charge was in error, the issuing bank charges back the merchant bank by removing the previously credited amount of the invalid charge from the

---

124. *Broadway Nat'l Bank*, 775 F. Supp. at 125. This document was entitled the "Merchant Bank Program." *Id.* Under the Program, a merchant collected credit card sales slips in a sealed envelope and attached a tally of them on the outside. *Id.* The merchant delivered the envelope daily to Broadway, which would inspect the tally calculations but was prohibited from opening the sealed envelope. *Id.* Broadway credited the merchant's account for the amount on the tally and forwarded the package to Chemical. *Id.* Chemical then credited Broadway's account and processed the slips through the network; for charges made on a Chemical-issued card, the network charged Chemical for the individual purchase amounts, and Chemical billed the cardholder. *Id.*

125. *Id.*

126. *See* Citizens & S. Nat'l Bank v. Thomas B. Hamilton Co., 969 F.2d 1013, 1015 (11th Cir. 1992); *Broadway Nat'l Bank*, 775 F. Supp. at 125. Billing errors include charges that appear on a cardholder's statement for items or services the cardholder did not purchase or receive, for amounts that do not coincide with the prices of the items or services the cardholder purchased, or for which clarifications are requested by the cardholder, including evidence of a purported transaction. *See* 15 U.S.C. § 1666(b) (1994); *Citizens*, 969 F.2d at 1015-16; 12 C.F.R. § 226.13(a) (1995).

127. *See* 15 U.S.C. § 1666(a); *Citizens*, 969 F.2d at 1015; 12 C.F.R. § 226.13(b)(1).

128. *See Citizens*, 969 F.2d at 1016. In the previous example, a contested charge would be returned by the issuing bank (if it was not Chemical) to Chemical. *See Broadway Nat'l Bank*, 775 F. Supp. at 125. Chemical would then attempt to reprocess the slip. *See id.* If unsuccessful on this attempt, Chemical would "charge back" Broadway's account for the contested amount. *See id.*

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 26 1996

merchant bank's account.[129] The cardholder is then discharged from the duty of paying for the improper charge.[130] Moreover, depending on the agreement between the merchant bank and the merchant, the merchant bank usually may charge back the merchant, thereby relieving itself from bearing the loss.[131]

An example of a merchant-merchant bank agreement that contains provisions addressing the parties' charge back rights is described in *Citizens & Southern National Bank v. Thomas B. Hamilton Co.*[132] The merchant, Thomas B. Hamilton Co., contracted with its bank, Citizens & Southern National Bank, and agreed to a provision which permitted the bank to shift a charge back to the merchant.[133] Paragraph eleven of the agreement enumerated the situations in which the bank could shift a charge back to the merchant:

> 11. [Hamilton] agrees to pay [C & S] the net amount of any sales draft, and [C & S] shall have the right at any time to charge [Hamilton] therefor without notice, in any situation relating to any such sales draft where: (a) merchandise is returned, or claimed to have been returned by customer, or services are rejected, whether or not a credit voucher is delivered to [C & S]; (b) any sales transaction exceeds the dollar limitation of the Card and has not otherwise been specifically authorized by [C & S]; (c) the sales draft is alleged to have been drawn, accepted or endorsed improperly or without authority; (d) the sales draft is illegible; (e) the Cardholder disputes the sale, quality or delivery of merchandise or the performance or quality of services covered by the sales draft, and (Hamilton) fails to resolve such dispute with the

---

129. *See Broadway Nat'l Bank*, 775 F. Supp at 125. The issuing bank is required to complete its investigation and deliver its findings to the cardholder within 90 days of receiving the contested charge notification. 15 U.S.C. § 1666(a); *Citizens*, 969 F.2d at 1016; 12 C.F.R. § 226.13(c),(e)-(f).

130. *Citizens*, 969 F.2d at 1016.

131. *Id.*

132. 969 F.2d 1013, 1016-17 (11th Cir. 1992). In *Citizens*, the merchant, Thomas B. Hamilton Co., entered into an agreement with Citizens & Southern National Bank whereby Hamilton was permitted to accept MasterCard and VISA credit cards for purchases made by its customers. *Id.* at 1014. Citizens would then accept the resultant charge slips from Hamilton for deposit and process them through the transaction network. *Id.* at 1014-15.

133. *Id.* at 1016.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 27 1996

> Cardholder; (f) the sales draft is drawn by or credit is given to [Hamilton] in circumstances constituting a breach of any term, condition, representation, warranty, or duty of [Hamilton] hereunder; (g) the extension of credit for merchandise sold or services performed was in violation of law or the rules or regulations of any governmental agency, federal, state, local or otherwise; or (h) the Card honored is invalid, expired, or listed on any current Hot Card or Restricted Card List, or [Hamilton] has been notified that credit card privileges have been revoked.[134]

The CH's obligation to pay IB is based on the card holder contract with IB, which is usually written by IB. IB's obligation to pay MB is a function of the by-laws of the Visa or other bank credit card organization. MB's obligation to pay M is based on the depositor agreement between MB and M. This chain of contractual obligation, which assures M of payment if it is not interrupted, parallels a direct contractual obligation from CH to M that is extinguished only by actual payment to M.[135] The critical analytical elements in this chain of contractual obligation are the preconditions to the obligation between MB and IB, and whether there is a non-recourse provision in M's contract with MB.

Suppose U is involved in an unauthorized use. U would present to M a credit card number actually belonging to CH, and receive goods or services after M obtained the authorization code. As usual, M would pay MB, MB would pay IB, and IB would present the fraudulent record of charge to CH in a monthly statement. CH would discover that she did not use the card in that transaction and would refuse to pay. IB would seek recourse from MB, who, in turn, would seek recourse from M. However, M usually cannot find U. The legal question is who bears the loss in this circumstance.

---

134. *Id.* at 1016-17. "The arrangement between C & S and Hamilton is typical of arrangements between all types of merchants and financial institutions that deal in credit card transactions." *Id.* at 1017.

135. *But see In re* Charge Card Servs., Ltd, [1988] 3 All E.R. 702, 708 (Ct. App.) (stating that purchaser's obligation to mechanic for services was extinguished by acceptance of credit card charge, even though issuer defaulted on its redemption obligation).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 28 1996

V. STEPS IN INTERNET PAYMENT TRANSACTIONS

When the credit card process is made electronic, there are several distinct messages: the message containing the credit card number flowing from U or CH to M, the credit card number, and additional ROC information flowing from M to IB, the responsive authorization code flowing from IB to M; the flow of goods or services from M to CH or U; the flow of the ROC from M to MB, from MB to IB, and from IB to CH; and, the payment order message from CH to IB, the payment order from IB to MB, and the payment order from MB to M.[136]

At this point, a comparison between credit card transactions and "cybercash" or "electronic cash"[137] transactions is appropriate. CH[138] can obtain cybercash in the form of one or more electronic tokens from IB[139] in exchange for cash paid by CH to IB, or a debit against an existing deposit account CH has in that bank. CH or U can exchange the cybercash for goods or services by transferring it to M. M can either spend the cybercash with another seller of goods or services (in which case M's situation would become identical to CH's situation) or present the cybercash for redemption through a clearinghouse arrangement similar or identical to the credit card clearinghouse arrangement. In simplified terms, M would present the cybercash to MB and MB would redeem the cybercash from IB. The steps in the cybercash

---

136. The order of description of the payment orders is the reverse of their chronological sequence. M receives conditional payment from MB upon presenting the record of the credit card charge. Then IB pays MB, usually through a clearance process. Finally CH pays IB. Recourse and charge-back rules usually shift the risk of non-payment by CH ultimately to M.

137. One could substitute a comparison between conventional credit card transactions and analogies of cybercash, such as private banknotes, which are rare, for reasons explained *supra*, or traveler's check's or cashiers checks, which are common. Merchandise discount coupons are similar to these examples of quasi-money, except that they can only be spent on certain goods or services.

138. For convenience, the designations for cybercash participants are the same as for credit card participants. One can now think of CH as standing for "Cybercash Holder," rather than "Cardholder."

139. A later section of this paper explores whether the issuer of cybercash necessarily is a bank, or whether a non-bank can be the issuer. *See infra* notes 140-65 and accompanying text.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 29 1996

payment system are virtually identical to the steps in the credit card system, except that cybercash is more likely to be freely negotiable than a record of credit card charge.[140] Depending on how participants wish to deal with the risk of forgery of cybercash tokens, there may be an authorization step in the cybercash system corresponding to verification of a credit card. This would correspond to the token number and additional transaction information flowing from M to MB or IB, and an authorization code flowing from MB to M. Unless these two authorization messages are absent, the messages in the cybercash system are the same as in a credit card system. The following sections explain and evaluate the legal and technological infrastructure necessary to support these kinds of payment systems.

A. *Legal Infrastructure for Managing Forgery and Dishonor Risks*

Commercial law must respond to actual risks, thereby creating the framework within which appropriate private arrangements can be made to allocate risk. Since electronic payment systems, such as credit card transactions on the Internet and electronic cash systems, involve two kinds of risks, two kinds of legal and technological solutions should exist. The first type of risk is the risk of dishonor and the second is the risk of forgery or repudiation. NII technologies change the relative balance between these types of risk by increasing the risk of forgery and therefore also increasing the risk of repudiation, while leaving the risk of dishonor approximately the same. Thus, there is a commensurably greater need for both technological and legal innovation in the

---

140. The author has not been able to find any authority for the proposition that a record of credit card charge is a negotiable instrument. Indeed, the contents of a credit card charge do not satisfy the requisites of U.C.C. Article 3 for negotiable instruments. The usual credit card charge is in writing, but it is not in the form of an unconditional order to pay the bearer or "to the order of" the payee. Thus, it does not satisfy the requisites of U.C.C. section 3-104 concerning negotiable instruments. *See supra* note 65 and accompanying text. A cybercash token, on the other hand, could be designed to meet these requirements, as long as its electronic form does not defeat the requirement that the purported negotiable instrument be a "writing."

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 30 1996

infrastructure that protects against the risk of forgery, rather than in the infrastructure that protects against the risk of dishonor. These innovations may be achieved through an adaptation of negotiable instruments law. Technological innovation involves encryption, which is used for both privacy and authenticating purposes. The associated legal response involves the creation of an appropriate institutional infrastructure to support the encryption technology. The following sections address, first, the risk of dishonor, and second, the risk of forgery and repudiation.

B. *Risk of Dishonor*

Payment systems function because trading partners are willing to trust the promise of the issuer of some kind of token. Credit card systems work because merchants and merchant banks believe that the issuing bank will pay money to liquidate the debt represented by the credit card record of charge. Check systems work because merchants and presenting banks believe that the drawee bank will pay the check when it is presented. Currency systems historically only have worked when everyone believed that the issuer, private bank, or colonial government would redeem bank notes. One of the problems with the early bank note systems of currency was that traders and geographic areas of exchange were remote from the issuing bank, which found it difficult to assess the risk of dishonor. When a question of possible dishonor arose, the efficacy of currency was reinforced by making it legal tender. That is, each participant in the trading system is forced to accept it from another.

The high risk of dishonor could lead to merchants refusing to accept electronic payment. If the issuer of a credit card cannot be relied upon to pay the electronic credit card charge, or if the issuer of an electronic token in an electronic currency system cannot be relied upon to redeem the token, then the payment system would be impractical or, at best, would operate with sharp discounts at each transactional stage. From a functional standpoint, cybercash will work only if two types of participants are satisfied about two types of recourse in the event of dishonor. Both purchaser and merchant must be satisfied that each has a legal right to payment directly or indirectly by the cybercash issuer. Each must also be

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 31 1996

assured that some kind of fund exists to cover a claim against an issuer in the event of issuer insolvency or disappearance.

Unlike the risk of forgery, where the risk-management strategy is mostly technological and only peripherally legal, the strategy for managing the risk of dishonor is mostly legal and only peripherally technological. The essential legal response has two parts: first, to make sure that the issuer has a legally enforceable obligation to pay, and second, to make sure that issuers are not judgment-proof.[141]

The legal infrastructure can handle the risk of dishonor in several ways. The simplest approach is for existing banks to be the ones that issue cybercash. If that occurs, and if no one else issues cybercash, the existing scheme of banking regulation would give users of cybercash enforceable claims against nonpaying banks, and would also ensure the availability of funds to cover dishonored obligations, through mechanisms like the Federal Deposit Insurance Corporation (FDIC). Banking regulations and regimes typically make it illegal to engage in the business of banking without a license, usually referred to as a charter.[142] In addition, banking regulation statutes impose capital requirements to reduce the risk of dishonor. Finally, virtually all banking regulation schemes provide specialized reorganization procedures and deposit insurance. Moreover, the banking system not only addresses the risk of dishonor but also provides an existing clearinghouse mechanism so that the cybercash eventually can be redeemed by the issuing bank.

It may be inadequate, however, to rely entirely on traditional banking regulation as a legal response to the risk of dishonor. Even now, non-banks, such as American Express and Seven-

---

141. Issuers may be judgment proof either because they are insolvent, having issued more promises than they have resources to cover, or because they have left a court's jurisdiction and cannot be located.

142. Banking regulation thus has a sharper "bite" than credit card regulation and some other types of regulation of electronic payments systems. If a bank engages in business without obtaining the required regulatory approvals, it commits a crime or a statutory tort. In contrast, if one is a statutory credit card issuer, that statutory status simply changes the rights and duties as between issuer and cardholder and may provide certain default rules for contractual relationships.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 32 1996

Eleven stores, are involved in issuing tokens (traveler's checks and money orders) that are used like cash.[143] The legal infrastructure must deal with the possibility that an entity not presently doing business as a bank could issue cybercash. Addressing this possibility requires considering a number of interrelated issues such as: whether issuance of cybercash by a new enterprise not presently doing business as a bank would violate existing banking law; if it would, what steps are necessary to conform the cybercash issuance with existing banking law; if such issuance would not violate existing banking law, what new statutory, regulatory, or common law requirements would be appropriate to protect against the risk of dishonor.

Determining whether issuance of cybercash by a new enterprise not presently doing business as a bank would violate existing banking law requires considering four sources of law: federal and state statutes regulating banking, and federal and state statutes regulating credit card issuers.

The scope of federal banking laws has engendered much controversy in recent years, but most of the controversy has been focused on whether banks should be allowed to engage in non-banking businesses.[144] Less attention has been paid to the boundary between banking and non-banking when determining whether the scope of banking regulations should be expanded to include a particular activity. Another issue regarding the scope of banking regulation involves efforts by the Federal Reserve Board to regulate NOW accounts.[145] The availability of share drafts to consumers with brokerage accounts is also a source of controversy, although the fact that the brokerage has arranged for these

---

143. *See* U.C.C. § 3-104 cmt. 4 (1995) (stating that both banks and non-banks can issue traveler's checks and money orders); 6 HAWKLAND ET. AL., UNIFORM COMMERCIAL CODE SERIES § 4-403:13, at 392 (1995) (noting that American Express issues traveler's checks).

144. *See* CLARK & CLARK, *supra* note 96, ¶ 16.07[1] (describing effect of Title III of the Depositary Institutions Deregulation and Monetary Control Act of 1980, Pub. L. 96-221, 96 Stat. 211 (1980), which allowed depository institutions to provide checking accounts that pay interest).

145. *See* Board of Governors of the Fed. Reserve Sys. v. Dimension Fin. Corp., 474 U.S. 361 (1986) (rejecting effort to extend bank regulation to NOW accounts).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 33 1996

share drafts to be cleared through banks has meant that many banks have not opposed the practice before banking regulatory agencies.

Traditionally, federal banking statutes regulated only the "business of banking," without defining that phrase with any precision. Over time, the business of banking had come to be defined primarily by two types of activity: offering demand deposits and making commercial loans.[146] The commercial loan activity was important in distinguishing between banks regulated by the Federal Reserve Board and other types of financial institutions like Savings and Loan Associations.[147] The demand deposit criterion was more central to determining whether the business of banking was involved at all.[148] Intuitively, the demand deposit criterion is useful because it distinguishes a bank from a borrower. Borrowers usually agree to repay debts over a period of time, and usually the debts are subject to various conditions. The debt owed by a bank under a demand deposit agreement allows the lender, the depositor, to determine when the debt must be paid.[149]

This basic distinction, when applied to the probable practices with respect to cybercash, suggests that the issuer of cybercash is accepting demand deposits. Although there may be limitations on the issuer's obligation to redeem the cybercash from the original purchaser, it is difficult to conceive of how a cybercash system would work without an unconditional obligation of the issuer to redeem the cybercash upon demand by a third- party. This makes cybercash indistinguishable from a check, which is a typical way in which the depositor of an ordinary bank presents a demand for payment of the debt represented by the demand deposit.

Of the participants in electronic credit card transactions, only the issuer is likely to be subjected to regulation. Such issuers are subject to federal law providing rights to credit card holders and

---

146. *See id.* at 365-66 (reviewing controversy over definition of banking); discussion *supra* part III.

147. *See Dimension Fin. Corp.*, 474 U.S. at 370.

148. *Id.* at 369.

149. *See id.* at 368.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 34 1996

to many state laws regulating extensions of consumer credit.[150] Compared to banking regulation, these regulatory regimes are not very intrusive.[151] Originally limited to banks, the VISA network now allows non-bank issuers to be members.[152]

The constitutional limitations on state establishment of banks are not of central importance to the legal infrastructure for cybercash, except to eliminate one possible approach: state issuance of cybercash. On the other hand, the analytical framework for deciding what constitutes bills of credit is an appropriate framework for deciding what constitutes money and a starting point for considering how issuance of cybermoney might be regulated. The usefulness of anything as a medium of exchange (unless it has extrinsic value) is adequately framed by the Supreme Court's three-part inquiry in *Briscoe v. Bank of Kentucky*:[153] (1) Is there a commitment by the issuer to redeem? (2) Is there a fund to cover redemption? (3) Is the obligation to redeem legally enforceable?[154] Cybercash proposals, like actual instances of currency, differ from checks or money orders written on deposits. The distinction is that redemption of cybercash, currency and other instruments on which a bank is the drawer, come from the general funds of the bank. Personal checks, on the other hand, are paid out of a fund identified with the depositor who is also the drawer of the instrument.

Whether there is an obligation to redeem depends upon the issuer, since issuers remain free to avoid an obligation. The cybercash analysis becomes interesting, however, when an obligation apparently exists based on the reasonable expectations of the user of cybercash. Next in importance is the legal enforceability of the obligation, followed by the existence of a fund to

---

150. *See, e.g.*, LA. REV. STAT. ANN. §§ 9:3510 - 9:3576.23 (West 1991 and Supp. 1995).

151. *See* ILL. ANN. STAT. ch. 815, para. 140/2 (Smith-Hurd 1993) (restricting issuer charge backs to merchants); MICH. COMP. LAWS § 445.862(a) (Supp. 1995).

152. *See* SCFC ILC, Inc. v. VISA U.S.A., Inc., 819 F. Supp. 956, 962 (D. Utah 1993) (describing history of VISA network), *aff'd in part, rev'd in part*, 36 F.3d 958, 960-61 (10th Cir. 1994), *cert. denied*, 115 S. Ct. 2600 (1995).

153. 36 U.S. (11 Pet.) 257 (1837).

154. *Id.* at 302.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 35 1996

cover redemption. This might be a bond, or it simply might be the general assets of the issuer.

All three requirements could be satisfied without subjecting issuers of cybercash to banking regulation or to any other type of regulation other than general contract and bankruptcy law. For example, entry might not be restricted in the business of issuing electronic payment tokens, whether the business is modeled on credit cards or cash. The magnitude of the risk of dishonor is proportional to the size of the obligation, and to the length of the "float."[155] For example, a debit card system presents relatively little risk of dishonor to a merchant accepting the card because redemption is simultaneous with use of the token for payment.[156] Since electronic payment systems are faster than their paper-based counterparts, the float is shorter, and thus the risk of dishonor is decreased.[157]

If the government abstains from regulating this market, however, the payment system will not work, unless merchants and intermediary banks possess methods to determine if issuers are likely to honor tokens issued in their names. One possible way of performing this is to create private networks that are similar to the present-day VISA and MasterCard networks. Under this system, only members of the network are allowed to issue trademarked tokens (the credit cards with the trademark "VISA" or "MasterCard" on the card)[158] and only issuers meeting certain criteria

---

155. The length of time a payment token circulates in the economic system before it is presented for payment to the issuer.

156. Nevertheless, even after the issuing bank receives and satisfies a payment order authorized by a debit card, the issuing bank may still repudiate the payment order by charging it back under some circumstances. *See* Sherman v. First City Bank, 893 F.2d 720, 723-24 (5th Cir. 1990) (summarizing and quoting debit card charge back privilege).

157. *But see* Los Angeles Nat'l Bank v. Bank of Canton, 280 Cal. Rptr. 831, 838 (App. Ct. 1991) (noting that the check clearance chain among banks is appropriately described as a "high stakes game of hot potato").

158. *See* VISA Int'l Serv. Ass'n v. VISA Hotel Group, Inc., 561 F. Supp. 984, 986, 996 (D. Nev. 1983) (finding registered trademark infringement by hotel chain that used VISA for hotel services; referring to registered trademark numbers 1,071,114 for plastic cards, and 1,152,655 for traveler's checks).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 36 1996

are allowed to become members of the network.[159]

A fundamentally different approach would be to have certificate authorities represent that issuers have met certain predetermined criteria, perhaps one of several alternative sets of criteria representing a continuum from less security to more security.[160] The arrangement between issuer and certification authority would be essentially contractual, with risk shifting as appropriate to insurance in the form of insurance bonds.

These alternatives handle the risk of dishonor in the same way, regardless of whether the electronic payment system is modeled on a credit card or electronic cash system. In both instances, third-party certification is required (as a practical, not a legal, matter) to protect against the risk of dishonor.

There may be circumstances in which another approach may be acceptable. This approach would use the model now represented by American Express, Diner's Club, and cards issued by large corporations such as Sears Roebuck and General Motors. Here, no need for third party insurance or certification against the risk of dishonor is required because of issuer reputation. Of course, this model still would require protection against the risk of forgery with respect to the issuers.

From a policy standpoint, the most appropriate relationship between banking regulation and NII payment systems is uncertain. If issuance of cybercash is classified as banking, then the development of cybercash may be inhibited because entrepreneurs wishing to be issuers may not wish to qualify as banks. From that perspective, the best policy would be to narrow the scope of banking regulation.

There is another perspective, however, suggested by the second

---

159. *See* SCFC ILC, Inc. v. VISA USA, Inc., 36 F.3d 958 (10th Cir. 1994), *aff'g in part, rev'g in part* 819 F. Supp. 956, 962 (D. Utah 1993) (providing overview of membership rules), *cert. denied*, 115 S. Ct. 2600 (1995); Worthen Bank & Trust Co. v. National BankAmericard, Inc., 345 F. Supp. 1309 (E.D. Ark. 1972) (outlining VISA-predecessor and MasterCard-predecessor membership arrangements), *rev'd* 485 F.2d 119, 121 (8th Cir. 1973), *cert. denied*, 415 U.S. 918 (1974).

160. For a further discussion of certificate authorities, see *infra* notes 212-29 and accompanying text.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 37 1996

criterion for effective protections against the risk of dishonor, assurance of a fund from which payment obligations can be redeemed.[161] Banking regulations meet the criterion by stringent controls on bank solvency: capital requirements, lending restrictions, and deposit insurance, accompanied and reinforced by elaborate systems of inspection, audit, and examination. Such requirements work only because they are reinforced by restrictions on entry; that is, a kind of licensing system for banks.

While one could argue that the emergence of cybermoney entrepreneurs[162] suggests the need to license these entities in the same manner as banks are licensed, the success of non-bank credit card issuers is powerful empirical support for leaving cybermoney unregulated, at least with respect to the insolvency basis of the risk of dishonor. On the other hand, participants in cybermoney arrangements, like participants in credit card arrangements, need contract-based protection against dishonor. This protection has traditionally been found in negotiable instruments law, which, as U.C.C. section 3-305 explains, enhances the position of holders in due course vis-a-vis issuers through the concept of negotiability.[163]

In electronic payment systems, it may be difficult to assure that requirements for negotiability are satisfied. In order to be a negotiable instrument, the token must be in "writing" and must be "signed" by the maker,[164] implicating the search for ways that

---

161. *See* Briscoe v. Bank of Ky., 36 U.S. (11 Pet.) 257 (1837).

162. *See* David Bank, *Turning PCs into ATMs*, DALLAS MORNING NEWS, Feb. 7, 1995, at D1 (considering "digital cash" as the key to unlocking the Internet's full potential for commerce); Cortese & Holland, *supra* note 6, at 80 (stating that cybermoney will play an important role in improving Internet commerce); Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES, June 12, 1994, at F46 (suggesting that recent advancements in cryptography may allow "digital cash" to replace conventional money); Peter H. Lewis, *Computer Jokes and Threats Ignite Debate on Anonymity*, N.Y. TIMES, Dec. 31, 1994, at A1 (predicting that "digital cash" could become the basic currency for new forms of on-line shopping and commerce); Peter H. Lewis, *Getting Down to Business on the Net*, N.Y. TIMES, June 19, 1994, at C1 (describing "digital cash" as a requirement to assuage the security concerns of large commercial companies).

163. *See generally* U.C.C. § 3-305 (1995) (outlining defenses and claims in enforcing the obligation of a party to pay an instrument).

164. U.C.C. § 3-103(a)(6); U.C.C. § 3-104(a).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 38 1996

electronic messages meet the writing and signature requirements.[165]

Rather than redefining artifacts of a document-based payment system to accommodate electronic transactions, it may be better, as revised Article 8 of the U.C.C. has done, to provide for the relative position of holders in due course and issuers by excluding certain defenses against claims by the holder in due course.[166] Otherwise, existing negotiable instruments law seems to be an appropriate legal framework for cybermoney tokens.[167]

On the other hand, it may be desirable to close the gap between the position of the holder of a cybermoney token or traveler's check and the holder of a record of charge resulting from a credit card transaction. A typical record of charge does not qualify as a negotiable instrument because it is not written in the form of an unconditional promise to pay.[168] A credit card record of charge is generally excluded from Article 4, which regulates payment of "items" (such as checks) by banks, because it is not included in Article 4's definition of "item."[169]

C. *Risk of Forgery*

Most evaluations of electronic payment systems readily identify the risk of forgery by the purchaser of goods and services as a major risk that must be addressed before such payment systems can become a commercial reality.[170] Forgery can defeat both

---

165. *See* MICHAEL S. BAUM & HENRY H. PERRITT, JR., ELECTRONIC CONTRACTING, PUBLISHING AND EDI LAW ch. 6 (1991) (addressing ways in which electronic messages satisfy the statute of frauds and other signature and writing requirements).

166. *See* U.C.C. § 8-502 (stating that a rights holder is not subject to the defenses of conversion unless the rights holder had notice or was involved).

167. *See generally* Amelia H. Boss, *Current Issues in Electronic Data Interchange: Electronic Data Interchange Agreements: Private Contracting Toward a Global Environment*, 13 N.W. J. INT'L L. & BUS. 31 (1992); Note, *Consumer Protection and Payment Systems: Regulatory Policy for the Technological Era*, 98 HARV. L. REV. 1870 (1985).

168. U.C.C. § 3-104, discussed *supra* notes 65-71 and accompanying text.

169. U.C.C. § 4-104(a)(9).

170. Both of the major bank credit card associations have published standards for the use of their credit card systems in electronic commerce. *See* MasterCard, Secure Electronic Payment Protocol draft version 1.1 (Sept. 29, 1995), available

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 39 1996

contract and redemption expectations. The risk of forgery is indistinguishable from the risk of repudiation because repudiation is likely to involve an allegation of forgery where no forgery actually occurred. In an actual forgery, the purported purchaser says truthfully, "That is not my signature; it is a forgery." In a repudiation the purchaser falsely says, "That is not my signature; it is a forgery."[171] Unless the merchant who accepts the electronic payment can reduce the risk of either an actual forgery or a falsely alleged forgery, the merchant is not assured of payment.[172]

A technological infrastructure which protects against forgery has two branches: privacy and authentication. Privacy measures frequently involve network security, and seek to prevent someone from using networked facilities, like routers[173] and routing messages, to *obtain* unauthorized access to payment information such as credit card numbers. Authentication seeks to prevent unauthorized *use* of payment orders, such as credit card numbers. The two branches of security are related; one cannot use a credit card number without authority unless one has it. Frequently, one seeking unauthorized use takes advantage of flaws in network security to obtain one or more credit card numbers. Conversely, unauthorized access does not create any harm unless the person obtaining access subsequently engages in unauthorized use.

---

from http://www.mastercard.com [hereinafter "SEPP"]; VISA International, Secure Transaction Technology Specifications version 1.0 (Sept. 26, 1995), available from http://www.visa.com [hereinafter "STTS"]. Both identify payment information integrity and cardholder authentication as basic requirements for a workable system. SEPP § 3.2; STTS §§ 2.2-2.3. Both use public key encryption and the certification authority concepts from X.509 and RFC 1422. SEPP § 4.0; STTS § 4.3.

171. *See* Xanthopoulos v. Thomas Cook, Inc., 629 F. Supp. 164, 168-69 (S.D.N.Y. 1985) (rejecting the theory that the original purchaser of traveler's checks had faked a forgery and denying payment of traveler's checks to the acceptor who did not insist on a counter-signature in his presence).

172. This statement raises the question of who bears the ultimate risk of loss when a forgery cannot be proven. It assumes the seller, as the first person to accept the electronic payment, bears the risk.

173. Routers, also referred to as gateways, interconnect two computer networks. Gateways route data among the networks to which they connect. *See* DOUGLAS E. COMER, INTERNETWORKING WITH TCP/IP 489 (1991).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 40 1996

Most concerns regarding credit card numbers on the Internet relate to privacy. Privacy of credit card numbers communicated on the Internet is less than the privacy of the credit card numbers communicated orally on the telephone system. Screening and retrieval of an orally communicated credit card number requires a person to listen to the conversation, while screening and retrieval of a credit card number transmitted on the Internet can be computerized.[174] Access to telephone communication and to Internet packets requires physical access to the circuit used.

In the long run, widespread use of public key encryption[175] for digital signatures will relieve the need for privacy in electronic payment systems, because in such systems, it does not benefit a would-be forger to know the electronic signature or the digitally signed credit card number; she still cannot commit a forgery without the private key of the signer.

For a variety of reasons, the best approach to increase security for credit card transactions on the Internet is to provide application level security rather than relying on the Internet or TCP/IP protocols.[176] Even if one were willing to wait until changes to

---

174. The connection-oriented character of the telephone system also inherently provides a measure of authentication security. One authenticates a person or entity by dialing the telephone number assigned to that person or entity, confident that subsequent communications occur only with the telephone equipment assigned to that number. This feature of the telephone system can be used as a means of authentication, by "callback" features, but most credit card merchants operating by telephone do not do this; they simply accept the word of a caller that she is who she says she is, and that she is authorized to use the credit card number given. The connectionless character of the Internet removes that means of authentication. One has no way of knowing that packets purporting to be from a particular Internet address actually come from that address. *See* Raymond T. Nimmer & Patricia A. Krauthouse, *Electronic Commerce: New Paradigms in Information Law*, 31 IDAHO L. REV. 937, 945 (1995) (stating that authentication becomes more difficult in an electronic transfer because the system relies on automation rather than human actors: "signatures, visual, voice, or similar personal contacts are not applicable . . . we cannot rely on the varied means of personal identification supporting that identification").

175. For a further discussion on public key encryption, see CROSS-INDUSTRY WORKING TEAM, *supra* note 6, at § 5.4.

176. A protocol is a formal set of rules that govern the communications between computers. The Transmission Control Protocol/Internet Protocol ("TCP/IP") suite defines the communication between different computers on the Internet.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 41 1996

the IP or TCP standards are adopted and applied by the thousands of participants on the Internet, secure IP and TCP levels would not protect against the most prevalent risks, which involve people masquerading as credit card holders. Application level security protects against those risks and also does not depend on changes to the IP and TCP standards. In other words, application level security provides both privacy and authentication, while network level security provides privacy, but little authentication of human beings (as opposed to computer nodes). Therefore, application level security is the correct technological approach. With application level security, however, the responsibility is on the senders and receivers of messages to implement security. Application level security for credit card transactions on the Internet can build on EDI experience in two respects: (1) with respect to the basic technology used to place orders, acknowledge them and exchange credit information and authorization; and (2) with respect to legal analysis of where the risk resides, depending on system, design, and contract among system participants.[177]

The most appealing form of application level security available at the present time is public key encryption.[178] Public-key encryption uses two different keys for the same message, one of which can be made available to the public generally, and the other kept secret.[179] To ensure secrecy, the sender uses the recipient's

---

177. Many current credit card systems rely on the security inherent in the circuit oriented character of the telephone system. If a credit card is used to place a large order for merchandise to be delivered to an address different from the address that the issuing bank associates with that card holder, then the credit card network places a telephone call to the cardholder to confirm the order.

178. *See* Henry R. King, *Big Brother, The Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224, 229 (1995); Jeffrey Rothfeder, *Invasion of Privacy Includes Related Articles on Corporate Espionage, Personal Investigations, Tips for Protecting Privacy, Legal Rights*, PC WORLD, Nov. 1995, at 152 (stating that the "best procedure for encoding data, according to most security experts, is public-key encryption"); *see also* Jenevra Georgini, Note, *Through Seamless Webs and Forking Paths: Safeguarding Authors' Rights in Hypertext*, 60 BROOK. L. REV. 1175, 1215 (1994).

179. *See* King, *supra* note 178.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 42 1996

public key to encrypt the message.[180] The message is then inaccessible to anyone lacking the corresponding private key, which is possessed only by the recipient.[181] To authenticate a message and to guard against repudiation by the actual sender, the sender uses her secret key to sign the message.[182] Then anyone with that sender's public key can decrypt the message, but the public key will decrypt only signatures coming from that sender.[183] Digital signatures using public key encryption are an appropriate response to the risk of forgery. By authenticating the identity of the digital signer, they make it virtually impossible for a forger to pass himself off as someone else, and because they make forgery virtually impossible, they make repudiation based on a falsely alleged forgery impracticable.[184]

Most approaches to public key encryption envision one or more public key certificate authorities that would maintain databases, somewhat like conventional telephone directories, albeit in electronic form, that associate each potential sender with her public key.[185] It is possible, though, to corrupt the key authority, just as a crook could masquerade as a credit card company or issuing bank in order to confirm a credit card order. However, as the independence of the entities that must be corrupted increases, the difficulty for someone who wants to compromise security increases correspondingly. Thus, by adding additional independent verification institutions, security increases even if no single entity is completely trustworthy.

Technological and legal questions associated with the key certification process form the core of the infrastructure questions with respect to the forgery risk. The technological issues have

---

180. *See id.* Actually, for performance reasons, most systems of public key encryption encrypt a "session key" at this step. *Id.* The session key is used to encrypt and decrypt the message content. CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 5.4.

181. *See* CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 5.4.

182. *Id.*

183. *Id.*

184. *Id.* §§ 3.0, 5.2.

185. *Id.* § 5.4.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 43 1996

already been addressed by the Internet community,[186] but the legal issues are still being resolved. For example, Utah recently became the first state to enact legislation governing digital signatures.[187]

Digital signatures employing public key encryption technology protect against two types of forgery that concern participants in electronic commerce: spoofing of CH, and forgery or spoofing with respect to the issuer.[188] In other words, digital signatures protect not only against the unauthorized use of someone's credit card, but also against counterfeiters of credit cards (or cybercash tokens). The issuer is the person who is ultimately responsible for the promise of payment. Just as economic incentives exist to counterfeit currency, in which case the counterfeiter falsely represents himself as the United States government and receives goods or services for the forged token, so to exists an economic incentive to present an electronic token which falsely represents that it is backed by the credit of a third-party issuer. Digital signatures are an appropriate way of reducing this risk. The electronic payment token, whether resembling a credit card or cybercash, would be digitally signed not only by the presenter, CH (the purchaser of goods or services), but also by the issuer, IB. The person accepting the payment token, M, uses public key encryption to authenticate the identities of both the presenter and the issuer. There is no reason that the certification authority

---

186. *See* S. Kent, *Privacy Enhancement for Internet Electronic Mail: Part II Certificate-Based Key Management: RFC 1422* (1993) (defining architecture and infrastructure for authentication system based on public-key encryption techniques). Public-key encryption uses a pair of keys to control the encryption and decryption process. *See* CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 1.1, Glossary. The sender encrypts the message with the receiver's public key, and the receiver decrypts the message with her private key. *Id.*

187. Utah Digital Signature Act, UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1995), which took effect May 1, 1995, provides legal recognition to computer-based documents which are authenticated with a digital signature. This article later addresses whether the authentication standard defined by the Utah statute is compatible with RFC 1422. *See infra* part VII.A.

188. Issuer in this sense includes the issuing bank in the case of third party bank credit card transaction models and the issuer of tokens in the case of the cybercash model. *See supra* notes 131-34 and accompanying text for a model of credit card and cybercash transactions.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 44 1996

managing the public keys for presenters cannot also manage the public keys for issuers.[189]

If digital signatures based on public-key encryption are the appropriate technical solution to both types of forgery risk, then the law must provide a framework within which public key encryption can operate. That means that electronic payments law, covering essentially the same subject matter now covered by Articles 3, 4, and 4A of the U.C.C., must offer a regime within which private contract can define rights and obligations that allocate risk. The law must also utilize appropriate default rules and minimum standards to ensure adherence. The legal infrastructure must also be one in which an appropriate technological public key infrastructure can operate comfortably. While the CA function may be performed by the same entity that performs other functions in the present payment system and extends those payment system functions into the electronic environment, there are new risks associated with certifying public keys. The Science and Technology Section of the American Bar Association, like the Utah legislature, has begun to work out a legal framework for certification authorities.

D. *Risk Allocation Models*

There are several models for allocating risk in payment systems. Virtually all rely primarily on contracts to provide details, limiting statutory prescriptions to frameworks for contracting, default rules and presumptions, and holder-in-due-course and consumer protection. Article 3 of the U.C.C. covers negotiable instruments and other commercial paper, and is relevant to traveler's checks,

---

189. The issuer-forgery risk overlaps somewhat with the dishonor risk: one reason that an issuer might dishonor the payment order is that the payment order resulted from forgery of the issuer's authorization. Thus, it might be efficient for the CA managing public keys for issuers to associate an issuer with its public key, making forgery impracticable, and also to vouch for the issuer's reliability in honoring authorized payment orders. Alternatively, there are a number of bank rating agencies in operation today. These rating agencies could electronically certify the reliability of an issuer with respect to dishonor. Also, it is important to realize that the authentication of the issuer's obligation at the time of payment makes possible anonymous digital payment systems. *See* CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 5.4.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 45 1996

non-bank money orders, and thus perhaps to cybercash.[190] The Federal Reserve Board's Regulation E, regarding electronic fund transfers, governs fund transfers by consumers.[191] Article 4 of the U.C.C. governs personal checks and other instruments payable by banks.[192] Article 4A of the U.C.C. governs "wholesale" wire transfers.[193] The Consumer Credit Protection Act[194] governs consumer credit card arrangements.

Most of these general bodies of commercial law address the risk of forgery while also addressing other risks. Forgery is a universal defense to paying an obligation based on commercial paper or a credit card transaction. Thus, all payment systems must accommodate a forgery defense and must identify the participant upon whom the risk of forgery falls. Typically, the statutory default rules focus the risk on the participant best able to detect the forgery, such as the payee of a personal check.[195] Contractual arrangements usually focus risk in the same way: on the merchant to whom a credit card is presented or on the first person to cash a traveler's check.

These risk allocation rules are well established in commercial law and can be applied to cybercash and Internet credit card transactions, with only two major difficulties. First, a participant may not use the contemplated security technology. For example, though a payment order may be digitally signed, the recipient may not check the digital signature for integrity. Second, while a participant may use the security technology and obtain third-party verification of a digital signature, a forgery may nevertheless occur. For example, a public certification authority might

---

190. U.C.C. §§ 3-101 to -805 (1995).
191. 12 C.F.R. § 205 (1995).
192. U.C.C. §§ 4-101 to -504.
193. U.C.C. §§ 4A-101 to -507.
194. Codified at 15 U.S.C. §§ 1601-1666j (1994) and various other sections of 15 U.S.C.
195. The Electronic Funds Transfer Act uses a similar philosophy of risk allocation. It limits the liability of a consumer for an unauthorized electronic funds transfer to $50, unless the consumer has knowledge of circumstances that lead to the reasonable belief that an unauthorized electronic funds transfer involving the consumer's account has been or may be effected, and fails to notify the financial institution. *See* 15 U.S.C. § 1693g(a).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 46 1996

erroneously certify that a forger's key belongs to the purported cardholder or cybercash owner. Certain evolving EDI rules address the first question.[196] The Utah Digital Signature Act addresses the second.[197]

For the moment, suppose that CH is not a consumer,[198] and that CH and M have entered into an EDI trading partner agreement. M would receive an electronic purchase order signed "CH." CH and M previously would have agreed that an electronic document signed "CH" can be relied upon as coming from CH. Under the ABA's Model Trading Partner Agreement, para. 1.5, the party agreement makes it conclusive that CH is bound by the message, even if it was sent by forger U who had somehow found out the password, private key, or other necessary triggers for the signature "CH."[199]

Under the U.C.C. Article 4A approach, CH would be able to avoid liability by proving that the message actually came from U.[200] This might be worth little to CH because of the difficulty of identifying and proving that a hacker obtained the password or key and sent the message. Article 4A's approach also creates the possibility of collusion between CH and U. If U is insolvent or has left a court's jurisdiction, then CH can appear in court with an affidavit from U containing U's perjured testimony claiming he

---

196. The EDI model is also interesting because of the likelihood that tokens involved in both the credit card and cybercash concepts will resemble EDI transaction sets.

197. *See* UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1995) (setting up a voluntary system for licensing public key certification authorities).

198. Virtually all EDI law, in the United States and abroad, applies only to non-consumer transactions. EDI doctrine sidesteps consumer transactions for several reasons, some having to do with the politics of negotiating international model agreements. For present purposes, the main difference between merchant-to-merchant transactions and merchant-to-consumer transactions is that merchants are more likely to enjoy symmetrical bargaining power, while consumers are more likely to have weak bargaining power compared to merchants and banks with whom they deal. Thus, a legal regime intended to cover consumer transactions typically would leave less to agreement and put relatively more in substantive legal rules that are not variable by agreement.

199. Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange - A Report and Model Training Partner Agreement*, 45 BUS. LAW. 1645 (June 1990).

200. U.C.C. § 4A-203 (1995).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 47 1996

sent the message when, in fact, CH actually sent the message. This exemplifies the risk of repudiation. Moreover, the mere possibility of M not being able to avoid the risk of loss by trusting messages signed in accordance with the agreed upon protocol would cause M to be unwilling to trust the system.

Under the proposed United Nations Commission on International Trade Law (UNCITRAL) model statute on EDI, the basic rule would be that the agreement of the parties governs the transaction.[201] In the absence of agreement, or if there is an agreement with which CH or M does not comply, the noncomplying party can show that the risk of loss should be borne by the other.[202] For example, suppose CH and M agreed on a digital signature and CH sent a digitally signed message to M, but M did not use the technology to check the digital signature. M could avoid the risk of loss by proving that the message came from CH, but absent such proof, M would bear the loss.[203] Conversely, where CH has not used the digital signature, CH could avoid the risk of loss by proving that the message actually came from forger U.[204] The problem here, as identified by Professor Boss, is that CH may

---

201. UNCITRAL, created in 1966, has 36 members, who are elected by the General Assembly of the UN. *See* John P. Dietz, *Introduction: Development of the UNCITRAL Arbitration Rules*, 27 AM. U. COMP. L.J. 449 (1979). UNCITRAL has issued voluntary arbitration and conciliation rules (1976), a Convention on Contracts for the International Sale of Goods (1980), a Convention on International Negotiable Instruments (1990), and other documents pertaining to industrial plans and shipping rules. *See generally* George A. Zaphiriou, *Unification and Harmonization of Law Relating to Global and Regional Trading*, 14 N. ILL. U. L. REV. 407 (1994); Henry P. DeVries, *International Commercial Arbitration: A Contractual Substitute for National Courts*, 57 TUL. L. REV. 42 (1982).

UNCITRAL now is working on rules for government procurement contracts, "counter trade" (trades made in kind rather than in cash), standby letters of credit, and electronic funds transfers. *See* Gerald T. McLaughlin & Neil B. Cohen, *Credit Enhancement Mechanisms*, N.Y.L.J., Sept. 13, 1995, at 3.

202. *See* Nimmer & Krauthouse, *supra* note 174, at 946-48 (citing UNCITRAL, Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Communication Art. 11 U.N.Doc.A/CN.9/406 (1994)); *see also*, Raj Bhala, *Paying for the Deal: An Analysis of Wire Transfer Law and International Financial Market Interest Groups*, 42 KAN. L. REV. 667, 700 n.162 (1994).

203. *See* Nimmer & Krauthouse, *supra* note 174, at 947.

204. *See id.*

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 48 1996

be concerned about its own employees and insist that M use a certain level of security to protect against a risk that is theoretically, but not actually, under CH's control.[205] Then, if M is allowed to avoid the agreed upon security and to shift the risk of loss back to CH by proving that CH's employees engaged in misconduct, the parties have lost the benefit of their agreement.[206] Despite the utility of some EDI model agreements and statutes for risk allocation concepts, major differences exist between EDI as it has been practiced and electronic payment systems intended for open environments such as the Internet, where there is no reliable and convenient secure channel to exchange and share a single secret key with a trading partner. Traditional EDI involves pre-established arrangements between pairs of trading partners, in which there are many secure channels for exchanging secret keys for symmetric key encryption. But what the NII needs is something quite different; it needs a system in which sellers or buyers can conduct business with an essentially open class of trading partners unknown to them before the transaction occurs. Public key encryption is essential for this kind of commerce.

VI. TECHNOLOGICAL INFRASTRUCTURE: COMPARISON OF ELECTRONIC CASH, TOKENS, AND PAYMENTS IN THE NATIONAL INFORMATION INFRASTRUCTURE RFC 1422

A number of commercial lawyers and commentators on Internet technology have developed the basic technology infrastructure concepts for cybercash and electronic credit card transactions.[207] Privacy-enhanced messaging[208] is the ultimate foundation for both electronic credit card and cybercash systems because it possesses the commercially available technology to provide for authentication and the privacy of electronic payments messages.

---

205. *See id.*
206. *See id.*
207. *See* http://www.ipps.lsa.umich.ada/ipps/papers.
208. This is also known as privacy-enhanced mail or privacy-enhanced e-mail. The more general term of privacy enhanced messaging is used in this paper because a payment order is more comfortably thought of as a specialized message rather than mail.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 49 1996

Two documents crystallize some basic concepts. The first is Request for Comments 1422 ("RFC 1422") from the Internet Engineering Task Force, which defines the technological infrastructure for privacy enhanced messaging.[209] The second document was written by the Cross Industry Working Team ("XIWT"), a group of private companies developing recommendations for the National Information Infrastructure.[210] The XIWT document explains in general terms how cybercash might work.[211]

RFC 1422's basic approach is to establish a hierarchy of certification authorities ("CAS").[212] Each CA would maintain records linking public keys with their owners.[213] CAs would be responsible for using an extrinsic proof of identity before establishing such a record.[214] Higher level authorities called "policy certification authorities" ("PCAs") would maintain records linking CAs with *their* public keys.[215] Thus a person to whom an electronic payments token is presented could verify its digital signature by checking and obtaining the public key from the CA indicated on the token, could verify the integrity of that CA by checking with one or more PCAs, and so on, up through the hierarchy.[216] The public key records of the CAs also would contain additional information, such as expiration dates of keys.[217]

RFC 1422 was designed to be compatible with Recommendation

---

209. Steve Kent, *Privacy Enhancement for Electronic Mail: Part II: Certificate-Based Key Management*, Network Working Group Request for Comments 1422, February 1993 (hereinafter "RFC 1422") (available on the Internet RFC index at http://www.csl.sony.co.jp/rfc/index.html).

210. *See* CROSS-INDUSTRY WORKING TEAM, *supra* note 6.

211. *See id.*

212. RFC 1422, *supra* note 209, § 2 at 3.4.4.

213. *Id.* § 2, at 3.

214. *Id.* § 2, at 4.

215. *Id.*

216. In the Utah system, and in guidelines being developed by the Information Security Committee of the ABA Section on Science and Technology, a user of public-key encryption could append his public key certificate to his public key, automatically supplying both the public key and the certificate to a trading partner. The recipient need only check with a CA to check Certificate Revocation Lists ("CRLs"). Some trading partners, however, might prefer to obtain public keys and certificates from a third-party CA, to reduce the risk of spoofing.

217. RFC 1422, *supra* note 209, § 3.5.1.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 50 1996

X.509 of the International Telegraph and Telephone Consuyltative Committee (CCITT), "The Directory - Selected Attribute Types."[218] In addition, RFC 1422 establishes a key management[219] infrastructure.

XIWT's digital cash payment system differs significantly from RFC 1422. For example, XIWT's proposed system does not require a fixed network infrastructure, and can be accomplished using an intermittent network connection such as mobile appliances that use wireless networks.[220] RFC 1422, however, was designed for the Internet, which is a worldwide collection of interconnected computer networks. Nevertheless, XIWT's proposed digital cash payment system still contains some attributes of the system defined by RFC 1422.

Most importantly, XIWT recognizes that encryption, digital signatures, and a key management system are required to ensure security and privacy, and to prevent fraud.[221] XIWT also recognizes that any implementation of digital cash will require a CA to "(1) vouch for the legitimacy of distributed public keys and (2) certify and register ownership of the associated transaction devices."[222] XIWT also recognizes that the CA would require a hierarchical structure to perform the following functions:

1. set policies for issuing and distributing certificates;
2. set policies for verifying certificates; and
3. establish directories that contain certificates and certificate revocation lists ("CRLs").[223]

Expiration dates, CRLs, encryption, and CAs are other common

---

218. *See id.* § 1, at 1. The Internet Activities Board's ("IAB") goal in specifying RFC 1422 was to make RFC 1422 compatible with different protocol suites including TCP/IP and OSI. *Id.* § 1, at 2. A protocol is a "specified procedure or process used to achieve a specific and common result, such as a network communications message format." CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 6.0, glossary.

219. Key management is a "process by which keys are distributed to usage points while kept in a protected form by encryption." CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 6.0, Glossary.

220. *See id.* § 1.0.

221. *See id.* §§ 3.0, 5.2.

222. *Id.* § 5.4 (describing role of certifying authorities).

223. *Id.*

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 51 1996

system requirements of both XIWT's proposed digital cash payment system and RFC 1422. First, to mitigate risk and fraud, XIWT has proposed time limits on its electronic tokens with the user having to redeem the token prior to the expiration deadline.[224] The concept is analogous to the certificate expiration date field in an RFC 1422 certificate. The certificate is also only valid for a finite time.[225]

Second, XIWT recognizes that certain administrative controls are needed. One such control is maintaining watch "lists" of bad tokens which are maintained to facilitate the early interception of known fraudulent activities.[226] This concept is similar to the CRLs required by RFC 1422.[227]

While XIWT has not selected a specific implementation, a CA hierarchy based on RFC 1422 could plausibly satisfy the requirements of XIWT's digital cash payment system. RFC 1422 is a key management system based on public key encryption.[228] It contains a hierarchical structure that addresses all the functions XIWT believes are required to implement their digital cash payment system.[229] Although the implementation detail of XIWT's system must be defined, it appears that the system could be compatible with RFC 1422.

---

224. *Id.* § 4.3.

225. *Id.* The XIWT document does not provide many implementation details, therefore, a direct comparison to the expiration date of the RFC 1422 certificate is difficult to make. *See id.* For example, XIWT does not discuss how the expiration date will be implemented. *See id.*

226. *Id.* § 5.2.

227. *Compare id.* (briefly describing the need for administrative tracking of "bad tokens") *with* RFC 1422, *supra* note 209, § 3.4.1.3 (describing CRL validating process). Again, XIWT does not supply the implementation details required to make a more detailed comparison. *See id.*

228. *See* RFC 1422, *supra* note 209, § 2 (providing an overview of the RFC 1422 approach).

229. *Id.*

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 52 1996

VII. COMPARISON OF UTAH DIGITAL SIGNATURE LEGISLATION AND RFC 1422 COMPATIBILITY

A. *Utah Puts into Law Concepts from RFC 1422: Public Key Certification*

The Utah legislation translates into law the basic public key certification concepts from RFC 1422 that prescribes the entities in a privacy enhanced E-mail system based on public-key encryption.[230] Both RFC 1422 and the Utah statute are based upon the common framework of X.509. The Utah Digital Signature Legislative Facilitation Committee drafted the digital statute to give legal effect to several standards, including both X.509 and RFC 1422.[231] It is important to understand that the Utah statute does not attempt to make digitally signed electronic payments legal tender.[232] Utah's statute has two optional elements: (1) it makes licensure of CAs optional,[233] and (2) it allows trading partners to use paper or to make any other form of payment arrangements they wish.[234]

Nevertheless, the Utah statute does contain additional requirements. For example, the format of the certificate[235] is different. The Utah statute has added the following additional fields to the certificate in order to address certain legal concerns:

1. subscriber's name;

---

230. UTAH CODE ANN. §§ 46-3-101 to -504 (Supp. 1995) (codifying the Utah Digital Signature Act as of May 1, 1995).

231. *See id.* ("This chapter shall be construed liberally to effectuate the following purposes: . . . (4) to give legal effect to the general import of the following and other similar standards: (a) Standard X.509 of the International Telecommunication Union (formerly CCITT or International Telegraph and Telephone Consultative Committee); (b) Standard X.9.30 of the American National Standards Institute (ANSI); and (c) RFC 1421 through 1424 of the Internet Activities Board (IAB).").

232. As sections 46-3-102(4)(a)-(c) of the Utah Code explain, any such attempt by a state would be preempted by federal law.

233. *Id.* § 46-3-201(5).

234. *Id.* § 46-3-201(6).

235. A certificate is a computer-based record which identifies a subscriber and contains the subscriber's public key. *Id.* § 46-3-103(4)(a).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 53 1996

2. subscriber's distinguished name;[236]
3. subscriber's public key;
4. brief description of any algorithms with which subscriber's public key was intended to be used;
5. certificate's serial number;
6. certificate's issued date;
7. certificate's expiration date;
8. distinguished name of the certification authority (CA)[237] issuing the certificate;
9. brief description of algorithm used to sign certificate;
10. recommended reliance limit for transactions relying on the certificate.[238]

Fields one through eight are required in both RFC 1422 and X.509. Field nine is required in the proposed working draft of an extended X.509 certification specification, but is not required in RFC 1422. Field ten is unique to the Utah statute and was added to provide the legal and institutional support required for digital signatures. The recommended reliance limit in field ten notifies merchants of the monetary limit of the CA's liability for errors.

The authentication hierarchy established by the Utah statute conforms to the authentication hierarchy of RFC 1422. The Utah statute establishes an administrative agency to regulate the authentication of computer-based documents.[239] This agency is analogous to the PCAs[240] in RFC 1422.

According to RFC 1422, a PCA is a certification authority that establishes and publishes policies that govern individual CAs. The

---

236. A distinguished name is a sequence of alphanumeric characters uniquely identifying the subscriber. *Id.* § 46-3-103(12). In some cases, the distinguished name might be the same as the subscriber's name. In most cases, however, the subscriber's name would be the name as people would know it, for example "Henry H. Perritt, Jr., Professor of Law," while the distinguished name would be unique and computer readable, for example "hperritt."

237. A certification authority can issue one or more certificates. *Id.* § 46-3-103(5).

238. *Id.* § 46-3-104(1)(j).

239. *Id.* § 46-3-204(2), -103(11).

240. A Policy Certification Authority establishes and publishes policies for registering CAs and subscribers. RFC 1422, *supra* note 209, § 1, at 3. For the Internet community, PCAs published their policies in the form of informational RFCs. The Utah statute would therefore be analogous to an Internet informational RFC.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 54 1996

PCA specifies the procedures used to verify each subscriber's identity and public key, and restricts the maximum validity interval for certificates.[241] In addition, the PCA is required to define the procedure for distributing Certification Revocation Lists (CRLs).[242]

Under the Utah statute, all the PCA functions described above are performed by the Division of Corporations and Commercial Code within the Department of Commerce.[243] This state administrative agency promulgates rules governing CAs,[244] and also acts as a CA.[245] The Division of Corporations and Commercial Code maintains a repository containing all certificates published by licensed CAs,[246] a certification revocation list,[247] a list of all licensed CAs and their public keys, and a list of all CAs whose licenses have been suspended or revoked.[248] In addition, at a minimum, the Division of Corporations and Commercial Code must specify the hardware and software requirements for each CA,[249] and must approve the encryption[250] techniques used to sign certificates.[251] Also, consistent with a PCA under RFC 1422, the Division of Corporations and Commercial Code has the authority to suspend or revoke the license of a CA.[252] Therefore, the authentication hierarchy of the Utah statute can be subsumed into RFC 1422.

---

241. *Id.*
242. *Id.* § 3.4.2.5.
243. UTAH CODE ANN. §§ 46-3-103(11), -501(1)-(5).
244. *Id.* § 46-3-501(4)(a).
245. *Id.* § 46-3-501(1)(a).
246. *Id.* § 46-3-501(2)(a).
247. *Id.* § 46-3-501(2)(d).
248. *Id.* § 46-3-501(2)(c).
249. *Id.* §§ 46-3-501(5)(a)-(b).
250. Encryption uses "ciphers to alter information before it is transmitted over a network." CROSS-INDUSTRY WORKING TEAM, *supra* note 6, § 6.0 glossary. It "ensures to the greatest extent possible, that messages cannot be read or altered during transmission." *Id.*
251. UTAH CODE ANN. § 46-3-501(4)(b).
252. *Id.* §§ 46-3-201(4)(a), -204(4).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 55 1996

B. *Legal Implications of Utah Statute: Managing Certification Authority Risk*

The Utah statute goes further than RFC 1422 in allocating risk of a CA mistake. CAs wishing to be licensed in Utah must post a bond, and their liability in the event of a mistaken certification is limited to the amount of the bond.[253] Other limitations on liability may be specified in special fields of CA records.[254]

The Utah statute is an appropriate model for other states to reinforce the legal infrastructure for managing the risk of forgery. By clarifying the legal effect of a digitally-signed message, it reinforces private means of contracting for payment among consumer, merchant, and banking institutions.[255] By defining the legal responsibility of CAs,[256] the statute enhances the ability of the technological infrastructure defined by X.509 and RFC 1422 to fulfill its role in reducing the risk of forgery and repudiation.

VIII. INTERNATIONAL DIMENSIONS

The Internet is a global phenomenon, and any assessment of the infrastructure for electronic payments in the Internet that ignores the international dimension is seriously incomplete. Electronic payments involving legal persons from different countries are adequately accommodated by the technological infrastructures proposed to deal with the risks of forgery. A digitally signed payment token can cross national boundaries just as easily as it can stay within national boundaries. A request for a public key certificate from a foreign CA works identical to a request for a public key certificate from a domestic CA.

Legal infrastructure concepts based primarily on national legal systems are inadequate for almost every party involved. Banking regulation, the most mature aspect of the legal infrastructure designed to deal with the risk of dishonor, is based almost entirely

---

253. *See id.* § 46-3-201(1).
254. *Id.* §§ 46-3-201(1)(f), -308(1).
255. *See, e.g.*, § 46-3-202 (outlining method of auditing CAs).
256. *See supra* note 252 and accompanying text.

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 56 1996

on national rules and statutes.[257] Indeed, banking regulators have been largely frustrated in their efforts to subject foreign banks to domestic regulation and to regulate monetary instruments issued by foreign issuers.[258]

Even if banking regulation based on the United States's model is the desirable way to protect against the risk of dishonor, it is impracticable to extend it internationally. Barriers are imposed by constitutional and statutory limits on the assertion of personal jurisdiction,[259] limits on extraterritorial application of American law,[260] other uncertainties with respect to choice of law,[261] and uncertain enforcement of civil monetary judgments and injunctions in foreign countries.[262]

Private clearinghouse agreements, such as those already in place to link banks and to handle credit card transactions, are the best institutional arrangements to manage both forgery and dishonor risks for payment systems in the Global Information Infrastructure (GII). Such private institutional arrangements can handle choice-of-law, jurisdiction, and dispute resolution better than nationally-based public law systems.

On the other hand, international arbitration agreements are widely respected by national legal systems.[263] Thus, any aspect

---

257. *See generally* Duncan E. Alford, *Basle Committee Minimum Standards: International Regulatory Response to the Failure of BCCI*, 26 GEO. WASH. J. INT'L L. & ECON. 241, 242-45 (1992).

258. *See generally* Andrew L. Strauss, *Beyond National Law: The Neglected Role of the International Law of Personal Jurisdiction in Domestic Courts*, 36 HARV. INT'L L.J. 373 (1995); Kurt Riechenberg, *The Recognition of Foreign Privileges in United States Discovery Proceedings*, 9 J. INT'L L. & BUS. 80 (1988).

259. *See generally* Anne-Marie S. Burley, *International Law and International Relations Theory: A Dual Agenda*, 87 A.J.I.L. 205 (1993).

260. *See id.*

261. *See generally* OKEZIE CHUKWUMERIJE, CHOICE OF LAW IN INTERNATIONAL COMMERCIAL ARBITRATION 107-08 (1994).

262. *See generally* Strauss, *supra* note 258.

263. *See* Mitsubishi Motors Corp. v. Soler Chrysler-Plymouth, Inc., 473 U.S. 614, 625 (1985) (rejecting presumption against arbitration of statutory claims because the contrary presumption applies in international arbitration and finding antitrust disputes to be arbitrable); Scherk v. Alberto-Culver Co., 417 U.S. 506 (1974) (stating that genuinely international arbitration agreement may provide for binding arbitration of statutory securities law claim); Convention on the

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 57 1996

of the legal infrastructure that relies on arbitration to enforce its norms is necessarily more practicable in the international payments system context.

This article has already observed how strong a role customary law and the law merchant tradition plays in the law of commercial paper under the U.C.C. It is but a small step to extend this into a broader concept of *lex mercatoria*[264] for application to international electronic payments transactions. The UNIDROIT substantive law principles are already available as a choice of substantive law, and international commercial arbitrators, which are highly regarded by commentators, are applying a brand of *lex mercatoria*, free of explicit roots in national legal systems.

Relying on arbitration for dispute resolution, and on *lex mercatoria* for substantive law to fill in the gaps of private contracts, is also consistent with the basic philosophy of conventional payments law and conventional payments practice, both of which look more to the parties as law makers than to statutes or administrative agency regulations as sources of substantive law.

IX. CONCLUSION

A GII modelled on the Internet can realize its potential only if payment systems can operate with the same convenience and safety familiar to merchants and consumers in today's credit card and 800-number catalog ordering systems. Reliable GII payment systems require technological and legal infrastructures to manage two types of risk: the closely coupled risks of forgery and repudiation, and the risk of dishonor by issuers of credit and currency equivalents.

The basic outlines are in place for an infrastructure to deal with the risk of forgery and repudiation. International standard X.509, the Internet Engineering Task Force's RFC 1422, the Utah Digital Signature Act, and the VISA and MasterCard frameworks are

---

Recognition and Enforcement of Foreign Arbitral Awards, June 10, 1958, 21 U.S.T. 2517, 330 U.N.T.S. 38 (codified at 9 U.S.C. § 201 (1994)).

264. *Lex mercatoria* means "the law-merchant," and is "[t]hat system of laws which is adopted by all commercial nations, and constitutes a part of the law of the land." BLACK'S LAW DICTIONARY 911 (6th ed. 1990).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 58 1996

compatible and make appropriate use of public-key encryption to authenticate payments in open network environments like the Internet. X.509 and RFC 1422, and parts of the VISA and MasterCard standards, define the technology, while the Utah act and other parts of the VISA and MasterCard standards define the legal framework for allocating risk. All that is needed for the system to flourish is for more states to enact legislation similar to the Utah statute, and for more certification authority enterprises to be established and to advertise their services so more consumers and merchants participate.

The infrastructure is less complete for the risk of dishonor. VISA and MasterCard assume that existing issuers of credit cards will play the same role in the new electronic environments. For those payment systems, the VISA and MasterCard networks provide technological security for the wire transfers involved, and allocate risk according to their private clearance and settlement bylaw contracts. The unanswered question is what legal and technological frameworks are needed for other types of issuers of electronic credit cards and cybercash: banks, enterprises such as CyberCash, Inc. and DigiCash, Inc., and other completely new enterprises that want to issue electronic credit cards or cybercash tokens.

Traditional banking regulation would not solve all of the potential problems. The development of credit card infrastructures alongside and outside traditional banking systems suggests that participants in payment systems do not need the assurance against dishonor that the regulation of banks offers to them. Prohibiting the introduction of new payment and credit tokens until the boundaries of bank regulation can be extended would stunt desirable development of the GII. Instead, market forces and the evolution of private clearinghouse mechanisms are the appropriate infrastructures to protect against the risk of dishonor. Not only are such mechanisms more adaptable to technological realities and faster to erect and administer, but they also can regulate effectively across national boundaries—something that conventional governmental systems have difficulty doing.

There are only two justifications for direct legal intervention through statutory law or agency regulation: a demonstrated

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 59 1996

problem non-redemption and dishonor, or a reluctance of consumers and merchants to accept new systems until more governmental protection is in place. Proponents of electronic payment systems that do not involve existing credit cards must pay more attention to this form of risk, or their payment schemes will not be widely accepted in the cybermarket. Ultimately, new payment systems primarily work because merchants and consumers are willing to accept them.

One other matter that the law must address is the protection of consumers and small merchants against overreaching by those that draft master payment system agreements, such as tomorrow's equivalent of today's credit card cardholder agreements and banking depositor agreements. The frameworks represented by the Federal Fair Credit Reporting Act, the Federal Electronic Funds Transfer Act,[265] U.C.C. Article 4A, Federal Reserve Regulations E and J, and model law on international credit transfers, adopted by the UNCITRAL in 1992,[266] are appropriate models. They leave the details to private contracting, while requiring disclosure and fair dispute resolution systems, and imposing limits on the magnitude of the risk that can be shifted to those with little bargaining power.

---

265. 15 U.S.C. § 1693a(6)(B) (1994) (excluding from the definition of electronic fund transfer, any transfer of funds not designed primarily to transfer funds on behalf of a consumer).

266. *See generally* U.C.C. Article 4A: Fund Transfers Pref. Note (1995).

HeinOnline -- 22 Rutgers Computer & Tech. L.J. 60 1996