The John Marshall Journal of Information Technology & Privacy Law

Volume 15
Issue 1 *Journal of Computer & Information Law - Fall 1996*

Article 4

Fall 1996

Allocating the Risk of Loss for Bank Card Fraud on the Internet, 15 J. Marshall J. Computer & Info. L. 39 (1996)

Randy Gainer

ALLOCATING THE RISK OF LOSS FOR BANK CARD FRAUD ON THE INTERNET

by RANDY GAINER†

I. INTRODUCTION

Demographers estimate that between thirty and fifty million people world-wide currently use the Internet.[1] Internet users increasingly use the Internet to make purchases. More than 25,000 merchants in 150 countries sell goods and services over the Internet,[2] and 32% of World Wide Web ("Web") users have purchased goods or services over the Internet.[3]

---

† Randy Gainer is an associate at Davis Wright Tremaine in Seattle, Washington.

1. *The CommerceNet/Nielsen Internet Demographics Survey: Executive Summary*, October 30, 1995 [hereinafter *"1995 CommerceNet Survey"*] (available on the World Wide Web @ http://www.commerce.net/information/surveys/exec_sum.html), as updated by *The CommerceNet/Nielsen Internet Demogrpaphics Recontact Study March/April 1996: Executive Summary*, August 13, 1996 [hereinafter *"CommerceNet Recontact Study"* (available on the World Wide Web @ http://www.commerce.net/work/pilot/Nielsen_96/ecec.html) (estimating that there are twenty-four million Internet users over sixteen years of age in the United States and Canada). *See also The Future of Money: Hearings Before the Subcomm. on Domestic and International Monetary Policy of the House Comm. on Banking and Financial Services*, 101st Cong., 1st Sess. 1 (1995) [hereinafter *Hearings*] (statement of William N. Melton, CEO, CyberCash, Inc.).

2. *Hearings*, *supra* note 1, (testimony of Heidi Goff, Sr. V.P., MasterCard Int'l.). Ms. Goff estimates that by the year 2000, more than one-hundred million people around the world will be connected to the Internet. *Id.*

3. *Internet Buyers in the Millions With Credit Cards Ready*, ON-LINE BUSINESS TODAY, Sept. 18, 1995, (newsletter No. 950918 [#11], available by e-mail at OBT@HPP.Com); Jeffrey Kutler, *Currency of the Internet Realm? So far, It's Plastic*, AMERICAN BANKER, Sept. 21, 1995, at 1 (reporting a survey by Verifone, Inc., MasterCard and Visa). The 1995 CommerceNet Survey estimated that of the 17,280,000 United States and Canadian Web users over sixteen years of age, 14% (2,419,200) had purchased goods or services over the Web. *Hearings*, *supra* note 1. The CommerceNet Recontact Study reported that in March/April 1996, the same percentage, 14%, of an increased number of web users had used the Web to purchase goods or services. *CommerceNet Recontact Study*, *supra* note 1. The CommerceNet Recontact Study also reported that, among people who use the Web for business purposes, more Web users sold products or services (increasing from 11% in 1995 to 16% in 1996) and more users purchased products (increasing from 24% to 30%). *Id.*

World wide Internet commerce revenues reached $350 million in 1995.[4] Credit cards are the payment method of choice for Internet shoppers.[5] Visa U.S.A. estimates that the volume of its Internet sales may match that of catalogue sales, which is fifty billion dollars in ten years.[6] Market researchers estimate that Internet sales may reach $300 billion by the year 2000.[7]

Despite the opportunities that the Internet presents as a new medium for sales, many merchants that advertise on the Internet, and many banks that issue MasterCard, Visa, and debit cards, caution consumers not to send their bank card numbers over the Internet.[8] Computer hardware and software vendors are competing to sell data encryption solutions to credit card companies, banks, and other businesses to protect financial transactions on the Internet.[9] Despite some set-backs,[10] MasterCard and Visa plan to authorize Internet transac-

4. Sebastian Rupley, *Digital Bucks? Stop Here*, PC MAG. May 28, 1996, at 54, (citing a study by Forrester Research).

5. Internet consumers were interviewed by Global Concepts, Inc., during May-August, 1995. The interviewees ranked credit cards as their first preference for making purchases on-line. *Id.* "Digital cash," checking account withdrawals, debit cards, and prepaid cards were the other means of payments listed by the consumers surveyed, in descending order of preference. *Id.* The survey results were similar to those obtained by MasterCard and Visa in less extensive surveys. *Id.*

6. Richard Bialek, Sr. V.P. of Consumer Credit and Products, Visa U.S.A., in May 23, 1995, address to the Washington Software Association, excerpted in the WSA News Bytes [on file with author]. This compares with 1994 total retail sales for Visa U.S.A. of $1.5 trillion, catalogue sales of fifty ($50) billion, and television/home sales of $2.5 billion. *Id.*

7. Russell Mitchell, *Safe Passage in Cyberspace: Theft-Proof Credit-Card Travel Means Cybertrade Can Take Off*, BUS. WK., Mar. 20, 1995, at 33.

8. *See, e.g.*, John T. Mulqueen, *Bankers See Internet as Risky Business*, COMMUNICATIONS WK. Apr. 10, 1995, at 1; Stephan Somogyi, *How Would You Like to Pay For That? A Guide to Digital Cash and Carry Technology*, DIGITAL MEDIA, Dec. 5, 1994, at 13 (stating that it is an invitation to disaster to transmit a credit card number in unencrypted form over a public network such as the Internet.).

9. Among the competitors are IBM; Cybercash, Inc.; Intuit, Inc.; Electronic Payment Services; Digicash, Inc.; Cybercash, Inc.; and VeriSign. *See Hearings*, *supra* note 1, (testimony of David Van Lear, Pres., EPS.; David Chaum, Chairman and CEO, Digicash, Inc.; William Melton, Chairman and CEO, Cybercash, Inc.; and Scott Cook, Chairman, Intuit, Inc.); *see also Beware: IBM Says Its Ready for Secure Cyberspace Commerce*, 18 EFT REPORT No. 13, June 21, 1995; *The Secure Net: Are We Almost There?*, ON-LINE BUSINESS TODAY, July 31, 1995, (newsletter No. 9500731 [#5], available by e-mail from OBT@HPP.COM).

10. Visa and MasterCard announced in mid-1995 that they would develop joint specifications for transmitting encrypted card data over the Internet. *See, e.g., Banks Get the Green Light to Hit the Internet*, 13 BANK NETWORK NEWS No. 4 (July 12, 1995) (stating that the announcements by Visa and MasterCard will encourage more banks and vendors to begin electronic commerce). Visa and its partner, Microsoft, announced their Secure Transaction Technology ("STT") in September 1995, while MasterCard and its partners Netscape Communications Corp., IBM Corp., Cybercash, Inc., and GTE Corp., posted draft specifications for their security measures on the World Wide Web in October. *See* Valerie

tions in 1996.[11]

While some observers are skeptical of claims that electronic commerce over the Internet is "set to explode,"[12] consumers are increasingly using bank cards to make purchases over the Internet. Until planned security measures for the Internet are proven to be effective, a question is raised: Who will pay for the loss if a criminal diverts bank card data used by a consumer over the Internet? This article discusses the risks associated with consumers' use of bank cards on the Internet and examines the statutory and contractual framework that will determine who bears the loss if Internet shoppers' card data are misused.

II. THE RISKS

The electronic transfer of funds is not new. People have sent money by wire transfer in the United States since the late nineteenth century[13] and have transferred money by telex for several decades. Even with the relatively secure "closed systems"[14] of wire-transfers and telex-orders, however, criminals have successfully diverted electronically transferred

---

Block, *Visa, Microsoft Catch Flack for Rushing Security Standard for Internet Payments*, AMERICAN BANKER, Oct. 2, 1995, at 1; Valerie Block, *MasterCard Posts Its Own Draft Security Standards for On-Line Payments*, AMERICAN BANKER, Oct. 6, 1995, at 12. The cracking of Netscape's encryption program by two University of California, Berkeley, students caused some Internet commerce observers to question the claims of those who contend that the Internet is safe for bank card transactions. Karen Epper, *Home Banking: Netscape Security Breach Causes Jitters*, AMERICAN BANKER, Oct. 3, 1995, at 18. *See also* John Markoff, *Security Flaw is Discovered in Software Used for Shopping*, N.Y. TIMES, Sept. 19, 1995, at A1. MasterCard, Visa and their respective partners resolved their differences sufficiently to agree February 1, 1996 on a joint software protocol, "Secure Electronic Transactions" ("SET"), for encrypting card data for transmission over the Internet. Jeffrey Kutler, *Despite Accord, Hard Work Ahead on Security Standard for Internet*, AMERICAN BANKER, Feb. 2, 1996, at 1, 14.

11. *Hearings*, *supra* note 1 (testimony of MasterCard V.P., Heidi Goff).

12. ON-LINE BUSINESS TODAY, *supra* note 9; *see also Bankers See a Goldmine in Sales Over the Internet*, 13 BANK NETWORK NEWS No. 4 (July 12, 1995). Even Internet commerce boosters acknowledge that security issues must be resolved. *Id.*; *see, e.g.*, Jeffrey Kutler, *Vendors Ready—And Waiting—For E-Commerce*, AMERICAN BANKER, Feb. 2, 1996, at 16. John Gould, MasterCard's vice president for electronic commerce, states: "MasterCard sees the Internet as having more impact on the way we live, communicate, shop, etc., even than the advent of television" but that "security is the 'biggest problem' facing on-line commerce." *Id.*

13. *See, e.g.*, *Hearings*, *supra* note 1, at 7 (supporting the remarks of David M. Van Lear); and BARKLEY CLARK & BARBARA CLARK, THE LAW OF BANK DEPOSITS, COLLECTIONS AND CREDIT CARDS, ¶ 16.05[1] at 16-33 - 16-34 (Rev. ed. 1995) (describing the high-value electronic funds transfer services operated by the Federal Reserve System (FEDWIRE), and by various banks (CHIPS and BANK WIRE), which together transfer hundreds of billions of dollars daily).

14. Rochelle Garner, *The Growing Professional Menance*, OPEN COMPUTER, July 1995, at 33, 40. These systems are "closed" in the sense that access to the telex and wire media used for the transfers is carefully controlled. *Id.* By contrast, anyone with a computer,

funds.[15]

The large-scale use of credit cards and the current use of debit cards at both automated teller machines ("ATM") and at Point of Sale terminals at retail outlets, increase both consumer convenience and opportunities for fraud. The fraudulent use of bank cards stolen from the mail, the manufacture of counterfeit cards, and other fraudulent uses of bank cards and card numbers cause banks to incur approximately $730 million in annual losses.[16]

The openness of the Internet creates an ideal environment for computer criminals.[17] The threat to computer security is no longer posed primarily by hackers who are intent on proving their technical expertise. The theft of all types of computer data results in losses estimated at ten billion dollars annually in the United States.[18]

Criminals actively trade and sell stolen credit card numbers on-line, and credit card issuers are one of the premier targets of on-line criminals.[19] These on-line thieves steal the credit card numbers and then sell them or merely post them on the Internet.[20]

---

modem and a dial-up access provider can gain access to the computers that the Internet uses to route data. *Id.*

15. In 1993, thieves forged telexes to the London office of Chase Manhattan Bank causing the bank to transfer $13.5 million in funds belonging to the Columbian government to the thieves' account. *See* BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE, § 4.2 at 46 (Supp. 1994). The forged telexes bore the correct "answerback" for the Columbian Central Bank, but omitted a "testkey" which Chase did not always demand for such transfers. *Id.* Another closed system for funds transfers, "remote banking" (which allows bank customers to access their accounts and transfer funds electronically from their telephones or personal computers), is also vulnerable, as the 1995 transfer by Russian criminals of $400,000 of other people's money to their own accounts showed. *See* Amy Harmon, *Hacking Theft of $10 Million From CitiBank Review*, L.A. TIMES, Aug. 19, 1995, at D1. The computer thieves attempted more than forty transfers, totalling more than ten million dollars, but after the first $400,000 had been stolen, the bank and the FBI discovered the attempts and apprehended six of the thieves. *Id.*

16. Kelley Holland, *Bank Fraud, The Old-Fashioned Way*, BUS. WK., Sept. 4, 1995, at 96 (noting that banks' losses due to check fraud (ten [$10] billion in 1991) dwarf all types of bank card fraud losses).

17. Amy Harmon, *Real Computer Threat Laid to Criminals, Not Hackers*, L.A. TIMES, Feb. 22, 1995, at A1.

18. Clinton Wilder, *On-Line Theft*, INFO. WK., Aug. 28, 1995, at 30.

19. *Id. See also* REPORT ON ELECTRONIC COMMERCE, Apr. 16, 1996, at 16 (reporting that five-thousand Visa Gold account numbers, stolen from a bank in South Dakota, were found on an Internet Service Provider's computer).

20. *See, e.g.*, Harmon, *supra* note 15, at D1 (describing the arrest of Kevin Mitnick, who allegedly stole twenty-thousand credit card numbers from Netcom Communications, a large Internet access provider, which had stored unencrypted card numbers on one of its servers); NEWSBITES NEWS NETWORK, Apr. 28, 1995 (1995 WL 2207231) (describing the German government's seizure of information stolen by a German data processing firm, including credit card information, belonging to eight million Germans and describing the posting by an Australian Internet user of a clear-text list of Internet users and their credit

The means by which cyber-thieves steal unencrypted bank card data is well-known and apparently not difficult for the thieves to accomplish. "Sniffer" software programs collect bank card data, as well as other valuable data such as log-in passwords for "secure" networks, at points where the data traverse high-traffic connections on the Internet.[21] One result is that the incidence of break-ins to computers attached to the Internet has increased at the rate of 73% per-year during the last two years.[22]

Encryption of bank card data, prior to transmission over the Internet, may diminish the risk that thieves will steal the data as it travels between consumer and Internet merchant.[23] There are other risks, as well. "The real risk on the Internet is the mass-theft of credit card numbers from merchants or organizations that have neglected server security."[24] That risk appears to be substantial.

---

card details, which he discovered on an Australian Internet service provider's server); *4 Held in Internet Shopping Spree*, CHI. TRIB., Mar. 19, 1995, at 22 (describing the arrest of four college students who obtained stolen credit card numbers over the Internet and used them to order $100,000 in computer equipment); and Susan M. Menke, *Electronic Highway: Men on the Attack*, GOVERNMENT COMPUTER NEWS, Apr. 3, 1995, at 20 (describing Ms. Menke's experience when thieves appropriated her Visa account number, which she had apparently used to pay her America OnLine access charge, and charged purchases to her account).

21. *See* Somogyi, *supra* note 8, 13. First Virtual Holdings, Inc., a company that sells non-Internet secure e-mail connections to facilitate electronic payments, demonstrated in January 1996 a "sniffer" program disguised a screen-saver program that was said to be readily available to computer criminals. *Id.* Karen Epper & Matt Barthel, *Warning About Internet Payment Security Raises Cries of 'False Alarm'*, AMERICAN BANKER, Feb. 1, 1996, at 18. The program could collect bank card data as the information was typed into a keyboard and subsequently transmit it to a criminal. *Id.* Reports also appeared that Java "Applets," used by many Web-site developers to add multimedia features to Web-sites, can be programmed to prompt Web-site visitors to re-enter log-in names and passwords and to transmit the data to the "Applets'" programmers. *See, e.g., Java: Be Afraid; Be Very Afraid*, ON-LINE BUSINESS TODAY, May 16, 1996 (newsletter, Vol. 2, no. 5, available through e-mail to OBT@HPP.Com).

22. Harmon, *supra* note 17, at A1. "The potential for significant disaster is there. We've got ourselves interconnected before securing ourselves." *Id.* (quoting Sandy Sparks of the Lawrence Livermore Laboratory who is Head of the Department of Energy's Computer Incident Advisory Capability).

23. The payment security schemes being developed by Visa, MasterCard and others are based on public key cryptography, a technology in which a combination of public and private cryptographic algorithms, or "keys," are used to encode and decode bankcard numbers and other sensitive financial data, that is sent between buyers and sellers. *See* Anne Knowles, PC WEEK, Oct. 30, 1995, at 104. The cracking of Netscape's security program suggests that it may take some time to develop and perfect sufficient encryption programs. *See* Markoff, *supra* note 10, at A1.

24. *Credit Card Companies Aim to Ease Consumer Fears but Visa, MC Standards Don't Deliver Total Security for Cybermarketers*, INTERACTIVE MARKETING NEWS, July 7, 1995, No. 14.

Security experts point out that computer criminals have managed to penetrate carefully protected United States Defense Department computer systems.[25] The problems with securing computer networks generally, especially those attached to the Internet, have caused some computer experts to conclude that "security is an illusion."[26] In other words, "[t]here is no such thing as perfect computer security. Security is not a destination; it is a journey."[27]

Even if bank card data are encrypted and authentication is automated through steps implemented by MasterCard and Visa, Internet based fraud will still cost companies an estimated one dollar for every one-thousand dollars of transactions conducted over the Internet.[28] Although this rate of fraud loss compares favorably to other technologies such as cellular phone fraud,[29] if the upper-end projections of Internet commerce are accurate, then approximately thirty million dollars in annual fraud losses relating to Internet transactions will occur.

III. HOW THE CURRENT STATUTORY AND CONTRACTUAL SCHEME ALLOCATES BANK CARD FRAUD LOSSES

A. CONSUMERS GENERALLY ARE NOT LIABLE FOR FRAUDULENT BANK CARD CHARGES

Two federal statutes generally prevent banks and credit card associations from charging consumers for losses incurred by the fraudulent use of bank cards. The 1970 amendments to the Federal Consumer Protection Act[30] (hereinafter *FCPA*) and the Electronic Funds Transfer Act of 1978[31] (hereinafter *EFT Act*) contain provisions that invariably pre-

25. Philip Shenon, *Defense Dept. Computers Face A Hacker Threat,* N.Y. TIMES, May 23, 1996, at A11, (citing a Government Accounting Office report which estimates that there were 250,000 attempts to penetrate Defense Department computers in 1995 and suggests that in 65% of those "attacks," the hackers were successful in gaining entry to the computer system); *see also* Rochelle Garner, *The Growing Professional Menace,* OPEN COMPUTING, July 1995, at 33, 36-38, (describing breaches of security conscious systems and a test by the Defense Information Systems Agency in which it broke into approximately 7,800 of the 8,900 Defense Department computers it attempted to penetrate); Curtis Lang, *Who's Spying Now?,* NETGUIDE, July 1995, at 44, 47 (noting that hackers have been able to penetrate Department of Defense "firewall-protected" systems using sniffer software).

26. Lang, *supra* note 25, at 50 (quoting Noel Matchett, former National Security Agency official and now President of Information Security, Inc.).

27. Benjamin Wright, electronic mail to LEXIS Counsel Connect listserve (transmitted June 18, 1995, 11:28 E.S.T.)(on file with the author).

28. PC WEEK, July 24, 1995, at 1.

29. *Id.* The rate of loss for cellular phone fraud is said to run at an annual rate of $20 of fraud loss to $1,000 in sales. *Id.*

30. Pub. L. No. 91-508, 94 Stat. 182 (codified as amended at 15 U.S.C. § 1643 (1994)).

31. Pub. L. No. 95-630, 92 Stat. 3728 (codified at 15 U.S.C. §§ 1693 to 1693r (1994)).

clude banks and credit card companies from charging consumers for fraudulent credit and debit card charges.

The credit card fraud section of the FCPA provides that a cardholder shall be liable for unauthorized credit card use only if: the card holder has accepted the card; the liability does not exceed fifty dollars; the card issuer gives the card holder notice of the potential liability; the issuer provides the cardholder with a description of the means by which the cardholder can notify the issuer of loss or theft of the card; the unauthorized use occurs before the card holder has notified the issuer of the loss or theft; and the issuer has provided a method by which the cardholder can be identified as the person authorized to use the card.[32] If a credit card holder asserts that a charge was unauthorized, the burden of proof is on the card issuer to show that each of these conditions has been met.[33] While the statute allows card issuers to impose liability up to fifty dollars, this is rarely attempted by lenders; thus this federal statute effectively eliminates cardholder liability for unauthorized use.[34]

The EFT Act establishes a similar comprehensive federal framework of consumer rights and liabilities for debit card transactions.[35] The EFT Act governs all "means of access . . . to a consumer's account for the purpose of initiating electronic fund transfers."[36] Regulation E[37] clarifies that "electronic fund transfers" include "all transfers resulting from debit card transactions, including those that do not involve any electronic terminal at the time of the transaction."[38]

The EFT Act[39] and the pertinent section of Regulation E[40] provide

32. 15 U.S.C. § 1643.

33. 15 U.S.C. § 1643(b). The same rules are restated in 12 C.F.R. § 226.12(b) (1995), part of Regulation Z, the Truth in Lending Regulations promulgated by the Board of Governors of the Federal Reserve Board.

34. CLARK & CLARK, *supra* note 13, ¶ 15.03[2][a] at 15-21. Many banks, apparently for customer relations reasons, do not attempt to assess the $50 limited liability charge authorized by 15 U.S.C. § 1643. *Id.* Reported cases suggest that banks may only attempt to enforce liability against a cardholder where there is an issue of real or apparent authority given by the cardholder to another to use his or her credit card. *Id.* at 15-21 to 15-23. If credit card data is stolen when used over the Internet, that data is an "unauthorized use" as defined by 15 U.S.C. § 1602(o) because the user will have no "actual, implied, or apparent authority for such use . . . ." *Id.*

35. *Id.* ¶ 16.06 at 16-54.

36. 15 U.S.C. § 1693a(1).

37. 12 C.F.R. § 205 (1996)(The Board of Governors of the Federal Reserve System issued Regulation E to implement the EFA Act).

38. 12 C.F.R. § 205.2(g). The primary objective of the EFT Act is "the protection of individual consumer rights." *See* 15 U.S.C. § 1693(b). Regulation E covers only consumer transfers; the rights and liabilities of parties to commercial wire transfers are governed primarily by Article 4A of the Uniform Commercial Code. *See* CLARK & CLARK, *supra* note 13, ¶ 16.06[1] at 16-56 n.102.

39. 15 U.S.C. § 1693g.

that a consumer's liability for unauthorized use of debit card data is generally limited to fifty dollars per incident or a related series of EFT transfers. There are some exceptions to this ceiling on liability. The first exception to the fifty dollar limit may occur if a consumer does not notify his or her financial institution within two business days after he or she discovers the loss or theft of an EFT card or Personal Identification Number.[41] In that instance, the consumer may be liable for up to 500 dollars of unauthorized use.[42] The second exception is that no ceiling on liability exists for unauthorized transfers if the consumer fails to notify the financial institution within sixty-days after the transmittal of a periodic statement to the consumer which shows the unauthorized transfers.[43]

Therefore, if consumer bank card information is stolen from an Internet computer protection from liability exists. This protection applies if the cardholder reviews his periodic statements and promptly notifies his bank of an unauthorized charge. The statutory limitations on consumer liabilities are included in the credit card/debit card agreements provided to consumers with their cards.

B. Merchants and Issuing Banks Will Pay the Costs for Internet-Related Bank Card Fraud

If consumers are not to pay the bill for fraudulent use of stolen bank card data, who will? If a merchant accepts bank card data for a sale without following the authorization procedures required by Visa or MasterCard and by the merchant's bank, only then does a merchant incur losses for accepting the fraudulent charge. On the other hand, the bank issuing the card bears the loss if stolen credit card data are used successfully by a cyber-thief, or by an individual who purchased a stolen card number from a cyber-thief, and no authentication procedures are violated upon card use.

This result is dictated by the contractual arrangements adhered to among bank card organizations, banks, and merchants. For example, the bylaws and operating regulations of MasterCard International and Visa U.S.A., Inc., contain the rules by which banks that issue credit cards and banks that process charges for merchants may "charge-back"

40. 12 C.F.R. § 205.6.

41. *Id.* § 205.6(b)(1).

42. *Id.*

43. *Id.* § 205.6(b)(6); *see also* Clark & Clark, *supra* note 13, ¶ 16.06[2] at 16-57. This unlimited liability "creates a strong incentive for customers to verify their monthly statements, just as Section 4-406 [of the UCC] creates a similar incentive where checks are involved." *Id.*

the charges between one another.[44] Neither Visa nor MasterCard currently have a standard that applies specifically to bank card purchases over the Internet.[45] Each credit card organization is in the process of considering new rules governing Internet transactions, but they do not yet have Internet-specific rules available. In the absence of Internet-specific authorization and charge-back rules, Visa and MasterCard use other rules by default. For example, Visa has rules regarding fraudulent mail and telephone transactions in which the cardholder denies participation.[46]

The situations in which merchants are required to absorb fraud losses for telephone orders and fraudulent Internet bank card orders are described in the standard terms bank card merchant agreements. Such agreements require merchants to strictly follow the bank card organization operating regulations. The regulations require details regarding a bank card sale to be electronically transmitted to the bank card organization's central authorization database, where the card data is checked for authenticity and to assure that the shipping address matches the cardholder's address.[47]

Standard merchant agreements require that merchants obtain central authorization regardless of whether an order is completed in person, over the telephone, or by mail order.[48] When the merchant obtains authorization an electronic code is transmitted to the merchant verifying that the card is valid and effective, and that the amount of the transaction is accepted by the central processing agency of the bank card organization.

Additionally, merchant agreements require merchants to warrant to their bank that the customer who presents bank card information is an authorized user of the card,[49] to authorize the bank to debit without notice a merchant's deposit account at the merchant bank when a con-

44. The bylaws and operating regulations of the credit card companies are confidential and may not be publicly disclosed without the permission of the bankcard organizations. The bylaws and operating regulations also govern settlement times, and minimum standards for charge authorizations among other rules.

45. Telephone Interview with Brian Rutter, Visa U.S.A. (Sept. 11, 1995); Telephone Interview with Caroline Cool, MasterCard International (Aug. 31, 1995).

46. Telephone Interview with Brian Rutter, *supra* note 45.

47. *See, e.g.*, Lisa Fickensher, *Fraud Losses Drop at Visa, Mastercard Series:1*, AMERICAN BANKER, May 24, 1994, at 1. Visa's "Payment Service 2000," a risk control system, is described as having reduced Visa's counterfeit card problem from 1992 to 1993. *Id.*

48. *See, e.g.*, *"Merchant Agreement,"* Bank of America, NW, N.A., doing business as Seafirst Bank (Feb. 1996), Section 6, "Merchant Procedures for Bank Card Transactions," subsection 6.03, "Authorization," and Section 6.10, "Telephone Orders, Mail Orders, Preauthorized Orders, and Recurring Transactions; No Imprint Procedures," subsection 6.10(A)(9), (requiring merchants to obtain an authorization code for each transaction).

49. *Id.* § 6.05(D).

sumer charges back a bank card payment sent for processing by the merchant,[50] and to require the merchant to indemnify the bank if the merchant violates the merchant agreement or the bank card operating regulations.[51] If a merchant accepts bank card data for payment without following the steps dictated in its merchant agreement, the merchant will bear the risk of loss if it ships goods or provides services in return for a bank card payment which turns out to be fraudulent.

C. New Encryption and Authorization Software Should Permit Secure Transmission of Card Data and Automated Verification of Account Status

In February 1996, Visa, MasterCard, Microsoft, IBM, Netscape, and other companies agreed to employ an industry-standard protocol for software to encrypt bank card data for transmission over the Internet. This protocol is a first step towards implementing an Internet payment infrastructure.

Software which will allow merchants who receive bank card data over the Internet to re-transmit card data to the card associations' central databases in order to obtain authorization codes is also needed, and is under development.[52] Testing of the software is to begin in June 1996 and commercial offerings for real-time verification, from consumers to merchants to banks, is scheduled for release in late 1996.[53]

IV. CONCLUSION

The computer software industry, payment system organizations, and the thousands of merchants investing in Web-sites sense that large numbers of consumers will use the Internet for commerce when consumers are convinced of this new medium's safe use. Consumers should not be concerned about potential theft of their bank card data, because federal statutes generally prevent the consumer from incurring liability for any significant misuse of the card data.

Most merchants and banks, on the other hand, are justifiably cautious when they discourage Internet shoppers from sending unencrypted card data for purchases. When software solutions are implemented to

50. *Id.* § 6.15, "Chargebacks."

51. *Id.* § 12, "Indemnification."

52. Jennifer Kingson Bloom & Jeffrey Kutler, *Two New On-Line Alliances Pair Niche Leaders*, American Banker, Feb. 21, 1996, at 1-14. Oracle Corp., in an alliance with Verifone, Inc., and Netscape Communications Corp., together with First Data Corp., are some of the companies that have recently announced their intent to provide Internet merchants with the equivalent of "card-swipe" authorization software. *Id.*

53. Kutler, *supra* note 3, at 14; *see also* Bloom & Kutler, *supra* note 52, at 14 (discussing Internet merchants intent to install software that will secure transmissions of card data).

adequately encrypt card data and to automate verification and authorization routines, payment technology will have caught up with the marketing potential of the Internet. At that point, risk of loss rules will protect merchants who follow contractually mandated verification and authorization procedures. Banks, the parties to Internet card transactions that may bear the largest percentage of Internet bank card theft, are likely to build enough margin into their processing rates to absorb the anticipated volume of challenged charges.

Once the planned encryption and verification "payment infrastructure" is installed and tested, realization of the potential for Internet commerce will occur. Statutory and contractual rules exist to protect consumers from card data theft and to allocate losses for whatever cybertheft that may occur.