Internet payment systems: Legal issues facing businesses, consumers and payment service providers

Robert F. Stankey*

The Internet is changing the way businesses sell everything from newspapers, music, groceries and airplane parts, to electronic equipment and natural gas. An increasing number of businesses are using the Internet to reach customers, process orders and receive payment with greater speed, at lower cost and in higher volumes than they could through traditional marketing channels. For example, Dell Computer Corporation increased its daily sales at its Web site from $1 million-a-day in January 1997 to $2 million-a-day in June 1997. Indicative of the medium's growth as a payment tool, Internet retail purchases of goods and services are expected to grow from between $500 and $600 million in 1996, to between $4 and $10 billion in 2000. Analysts expect that small value purchases will play an important role in the growth of retail sales on the Internet. Jupiter Communications predicts that 1.7 billion transactions, or 80 percent of all on-line transactions, will fall into the sub-$10 price band by 2000. Large volume billers, such as power utilities and telephone companies, are also expected to get more of their customers to pay their bills via the Internet.

Similarly, business-to-business transactions over the Internet represent an even larger market with an estimated $8 billion in transactions in 1997. By the year 2000, inter-company transactions are expected to grow to between $60 and $160 billion, allowing it to set its prices 10 to 15 percent lower than its competitors. See Christopher Anderson, In Search of the Perfect Market, The Economist, May 10, 1997, at 5-6 (separately paginated insert providing a graph indicating the projections of six analyst organizations). See also CyberAtlas/Retail (1997) <http://www.cru.com/research/retail.html> (analyzing the efficiency of Internet-based business-to-business commerce and reporting specifically that "[commercial users of the new medium] Millipore and 3Com have discovered that Internet-based orders can be processed more quickly, with fewer errors, at much lower cost and in higher volume than via phone and fax"). See also Steve Lohr, Business to Business on the Internet, N.Y. Times, Apr. 28, 1997, at D1 (reporting that GE Lighting, a subsidiary of General Electric Company, reduced procurement times by 50 percent and costs by 30 percent by purchasing over the Internet). Dell reports that those who visit the company's Web site prior to ordering over the telephone are 1.5 times more likely to make a purchase than those who do not. Erwin et al., supra note 2. See also Gary McWilliams, Whirlwind on the Web, Computer Maker Dell is Showing the World How to Run a Business in the Cyber Age, Bus. Wk., Apr. 7, 1997, at 132 (describing how the efficiency of direct sales over the Internet have contributed to Dell's success in reducing costs, although 53 percent of Internet users have decided on a purchase through the use of the Internet, only 15 percent report having actually made a purchase online. See CyberAtlas/Electronic Commerce, (1997) <http://www.cyberatlas.com/ecommerce.html> citing Anderson, supra note 4. This is at least partially a result of the low percentage of Web sites that offer online payment. See Anderson, infra note 13.

* Robert F. Stankey is Assistant General Counsel of Cyber Cash, Inc., Reston, Virginia.

1 For businesses that are offering these products on the Internet, see the following World Wide Web sites: www.mercercenter.com (newspapers), www.cdnnow.com (music), www.peapod.com (groceries), www.boeing.com/assocproducts/spares/home.html (airplane parts), www.cisco.com (electronic equipment), and www.quicktrade.com (natural gas).

2 See Blane Erwin et al., The Forrester Report, Sizing Intercompany Commerce (July, 1997) <http://access.forrester.com/index.../1997/reports/jul97tr.htm&q=6815> (analyzing the efficiency of Internet-based business-to-business commerce and reporting specifically that "[commercial users of the new medium] Millipore and 3Com have discovered that Internet-based orders can be processed more quickly, with fewer errors, at much lower cost and in higher volume than via phone and fax"). See also Steve Lohr, Business to Business on the Internet, N.Y. Times, Apr. 28, 1997, at D1 (reporting that GE Lighting, a subsidiary of General Electric Company, reduced procurement times by 50 percent and costs by 30 percent by purchasing over the Internet).

3 Dell reports that those who visit the company's Web site prior to ordering over the telephone are 1.5 times more likely to make a purchase than those who do not. Erwin et al., supra note 2. See also Gary McWilliams, Whirlwind on the Web, Computer Maker Dell is Showing the World How to Run a Business in the Cyber Age, Bus. Wk., Apr. 7, 1997, at 132 (describing how the efficiency of direct sales over the Internet have contributed to Dell's success in reducing costs, although 53 percent of Internet users have decided on a purchase through the use of the Internet, only 15 percent report having actually made a purchase online. See CyberAtlas/Electronic Commerce, (1997) <http://www.cyberatlas.com/ecommerce.html> citing Anderson, supra note 4. This is at least partially a result of the low percentage of Web sites that offer online payment. See Anderson, infra note 13.

4 See Christopher Anderson, In Search of the Perfect Market, The Economist, May 10, 1997, at 5-6 (separately paginated insert providing a graph indicating the projections of six analyst organizations). See also CyberAtlas/Retail (1997) <http://www.cru.com/research/retail.html> (analyzing the efficiency of Internet-based business-to-business commerce and reporting specifically that "[commercial users of the new medium] Millipore and 3Com have discovered that Internet-based orders can be processed more quickly, with fewer errors, at much lower cost and in higher volume than via phone and fax"). See also Steve Lohr, Business to Business on the Internet, N.Y. Times, Apr. 28, 1997, at D1 (reporting that GE Lighting, a subsidiary of General Electric Company, reduced procurement times by 50 percent and costs by 30 percent by purchasing over the Internet).

5 See Jupiter Communications Digital Commerce (1997) <http://www.jup.com/tracks/commerce/pricing.html>. However, a CommerceNet/Nielson survey found that although 53 percent of Internet users have decided on a purchase through the use of the Internet, only 15 percent report having actually made a purchase online. See CyberAtlas/Electronic Commerce, (1997) <http://www.cyberatlas.com/ecommerce.html> citing Anderson, supra note 4. This is at least partially a result of the low percentage of Web sites that offer online payment. See Anderson, infra note 13.

6 See Jupiter Communications Digital Commerce, supra note 5.


8 See Erwin et al., supra note 2. This represents a 1,000 percent increase from 1996. See id.
lion. For example, by July 1997, Cisco Systems, Inc. expected to sell network equipment from its Web sites at an annual rate of $2 billion. Also, in 1997, "[d]urable goods makers, chiefly in electronics and airplane parts, [are projected to earn $3 billion in revenues]-38 percent of all 1997 Internet business trade." As an example of its looming market impact, the Internet durable goods market alone is expected to increase to $99 billion by 2002.

By contrast, however, a minority of retail and business-to-business sites presently offer on-line payments. As more marketing and product ordering takes place on the Internet, more businesses will also want to accept payments directly at their Web sites, if only for convenience sake. Catering to what is perceived as increasing need, a variety of different technologies are available or are being developed to permit businesses to accept payments in this fashion. Generally, these payment technologies are based on one of three types of payment instruments - credit cards, debit instruments and digital currency.

This survey article compares and contrasts different types of existing and emerging Internet payment systems, and reviews the legal issues that are developing around them. The discussion is approached from the perspective of payment systems users, which include on-line merchants and purchasers, and likewise, the systems providers, financial institutions and non-bank service providers.

Part I of this article surveys credit-based payment systems on the Internet, and discusses liability issues and methods for error correction. Part II, in fashion, discusses debit-based payment systems, highlighting the newest iteration of personal debit transaction tools. Focusing on the newest form of Internet payment, digital currency, Part III of this paper discusses several emerging forms of on-line currency and some of the relevant legal and policy issues. This article concludes that the present growth of Internet-based payment systems as a market tool presents legislators with particular goals as they adapt existing law to comport with Internet use. Thus, the onus of businesses that adopt Internet payment systems will be to pay close attention to this emerging legal arena.

I. CREDIT-BASED PAYMENT SYSTEMS

Currently, most Internet payments are credit card transactions. However, the percentage of credit card transactions will likely decrease as Internet commerce grows. Nevertheless, credit cards are still expected to represent more than $8 billion in payments by 2000. Credit cards offer Internet shoppers the same conveniences and legal protections that they are accustomed to receiving when making credit card purchases by telephone or mail order. Therefore, before discussing credit-based systems on the Internet, it is useful to review the use of credit cards in the physical world.

A. Credit Cards in the Physical World

Traditionally, a merchant is paid by its own bank after the bank receives the credit card sales draft from the merchant. This bank is referred consumer Web sites and 3 percent of business-to-business Web sites conduct financial transactions at the site. See id.

10 See Lohr, supra note 2 at D1. By May, 1997, Cisco Systems, Inc.'s sales via the Internet had already reached $5 million per day ($1 billion annually). See id. Similarly, General Electric Company projects $1 billion a year in purchases over the Internet following its implementation in 1996. This implementation follows the successful Internet use by its subsidiary, GE Lighting, of a Web-based service linking corporate buyers and sellers. See id.

11 Erwin et al., supra note 2. By comparison, non-durable sales over the Internet are projected to total $182 million in 1997. See id.

12 See id. Non-durable goods sales are expected to reach $17 billion. See id.

13 See Anderson, supra note 4. Only 9 percent of consumer Web sites and 3 percent of business-to-business Web sites conduct financial transactions at the site. See id.

14 See Lohr, supra note 2, at D1 (reporting that Dell Corporation intends to ultimately handle all business transactions online).

15 See David E. Weisman et al., The Forrester Report, Payments on the Web (March 1, 1996) <http://access.forrester.com/index...eisman%27%29%3Aauthor&TYPE=reportX>. See id.

16 See id. Because this article focuses on Internet payment systems, legal issues relating to electronic commerce in general, such as the enforceability of electronic contracts, digital signatures, intellectual property, sales and income taxation, and jurisdictional matters, are not discussed.

17 See Weisman et al., supra note 15.

18 See id.

19 See id.


21 See id.
to as an “acquiring bank” because it “acquires” credit card transactions from the merchant.\textsuperscript{22} By contrast, the credit card holder's bank is referred to as the “issuing bank” because it issues the credit card.\textsuperscript{23} It takes from 90 to 120 days for the merchant’s acquiring bank to receive money from the issuing bank because the issuing bank generally does not transfer funds to the merchant’s bank until it receives payment from the cardholder.\textsuperscript{24} However, the acquiring bank pays the online merchant well before the issuing bank has settled with the acquiring bank.\textsuperscript{25} Consequently, the merchant’s acquiring bank has effectively extended credit to the merchant in the amount of the credit card payment.

As described in greater detail below, a cardholder can dispute a credit card transaction if, for example, the holder’s card has been stolen.\textsuperscript{26} If a cardholder disputes a credit card charge, the issuing bank will not pay the merchant’s bank and the merchant’s bank will reverse the transaction by processing a “charge-back” against the merchant’s account.\textsuperscript{27} Typically, the merchant’s bank will require the merchant to maintain a minimum balance in its bank account to insure that some money is available for charge-backs.\textsuperscript{28}

Acquiring banks make money by deducting a discount or settlement fee from the amount paid to merchants by cardholders.\textsuperscript{29} If a cardholder disputes a transaction and does not pay the acquiring bank, the bank does not receive its fee and incurs the cost of processing a charge-back against the merchant.\textsuperscript{30} Acquiring banks have learned that charge-backs more likely occur in transactions in which the cardholder does not present the card to a merchant in person.\textsuperscript{31} When the card is personally presented (in so-called “face-to-face transactions”), the merchant can verify the identity of the cardholder by checking the cardholder’s signature or requesting a driver’s license or some other identification.\textsuperscript{32} When the card is not personally presented, as with 800 telephone numbers and mail order sales, it is more difficult to verify the cardholder’s identity, and more likely that a stolen card is being used.\textsuperscript{33} Due to the greater risk of charge-backs, acquiring banks charge a higher discount rate for the so-called “mail order/telephone order” (“MOTO”) transactions where the actual card is not presented to the merchant.\textsuperscript{34} For example, an acquiring bank may charge 1 to 2.5 percent for transactions where the card is present but 2.4 to 5 percent for transactions where it is not.\textsuperscript{35}

Usually an acquiring bank hires a processor to receive and process credit card drafts from merchants.\textsuperscript{36} Processors receive credit card transaction data electronically from merchants through a private telephone connection. At the time of a transaction, the merchant sends a request to its acquiring bank’s processor to authorize the transaction. Depending on the processor, the transaction will be transmitted for settlement at the same time or later in the day. For this common transactional sequence, the merchant gener-
ally pays the processor a fee ranging from $0.25 to $0.70 per transaction, with certain monthly minimums.\(^{37}\)

B. Credit Cards on the Internet

Credit cards are used on the Internet to make payments in a variety of ways. Credit-based systems can be analyzed from two perspectives depending on whether the purchaser initiates authorization of a credit card transaction by transmitting data through a processor, or whether the merchant receives credit card data from the purchaser that the merchant then submits to its processor.

1. Merchant-Initiated Credit Systems

In a merchant-initiated system, a purchaser sends credit card information to a merchant either "in the clear" on the Internet, without the protection of any encryption, or using the secure sockets layer encryption ("SSL") that is available as a component of the major Internet browsers.\(^{38}\) The merchant transmits the credit card information to its processor by entering the information into software running on a computer.\(^{39}\) The data is then transmitted either via private telephone connection or the Internet.\(^{40}\) Transmission by means of the Internet involves sending the information over the Internet to a gateway computer server that sends the data to the merchant for processing.\(^{41}\) Internet merchants using these systems pay their acquiring banks the higher discount fee associated with the transactions in which the credit card is not present.\(^{42}\)

2. Purchaser-Initiated Credit Systems

In a purchaser-initiated system, a purchaser uses special software called a "wallet" to send credit card information to a merchant.\(^{43}\) The wallet encrypts the information with a greater level of encryption than is available in the major Internet browsers.\(^{44}\) The merchant transmits the credit card information in encrypted form over the Internet for processing.\(^{45}\) However, the merchant never gets access to the credit card information.\(^{46}\) Transmission by means of the Internet involves sending the information over the Internet to the gateway computer server that sends the data to the merchant for processing.\(^{47}\) Internet merchants using these systems pay their acquiring banks the higher discount fee associated with the transactions where the credit card is not present.\(^{48}\)

Visa and MasterCard have developed the Secure Electronic Transaction ("SET") protocol in order to provide a method for secure credit card transactions over open networks such as the Internet.\(^{49}\) In its full implementation, SET uses wallet software in the same manner as the purchaser-initiated systems to encrypt data in order to protect it from interception on the Internet, but adds the use of digital certificates to verify the identity of the cardholder.\(^{50}\) Merchants processing transactions using the full implementation of SET will likely pay the lower discount rate associated with face-to-face transactions.

C. Consumer Protection and Loss Allocation

The federal law and the credit card issuers’
rules define most of the significant rights and responsibilities of credit card users.\textsuperscript{51} The most important issue that these laws and rules address is who bears the cost of unauthorized credit card use. From the perspective of the credit card holder, these laws and rules provide a great benefit by limiting the holder's liability for unauthorized use and providing other protections designed to make it easier for the holder to challenge unauthorized transactions.\textsuperscript{52} Since no special regulations have been created for credit card use on the Internet, presumably the same laws and rules that govern credit card transactions in the physical world apply to Internet transactions. Consequently, the legal benefits protections, together with credit cards' ease of use and consumer familiarity, are some of the more important reasons that credit cards have become the most popular payment instrument for purchases on the Internet.

Federal Reserve Board Regulation Z,\textsuperscript{53} which was issued to implement the Truth in Lending Act,\textsuperscript{54} provides consumers with a variety of protections regarding consumer credit marketing and under what terms and conditions such credit may be provided.\textsuperscript{55} The provisions that are most significant for electronic commerce deal with liability limitations, error and dispute resolution, and disclosure.

1. Liability Limitations

Regulation Z limits a cardholders' liability for unauthorized credit card transactions at $50.\textsuperscript{56} The agreement that a merchant signs with its acquiring bank permits the acquiring bank to process a charge-back against the merchant in the amount of the unauthorized payment.\textsuperscript{57} The credit card issuers or their associations, such as Visa and MasterCard, have detailed rules and procedures governing when acquiring banks can institute charge-backs against merchants.\textsuperscript{58} Nevertheless, merchants bear the same high risk of fraud when accepting credit cards on the Internet, as they do in the physical world.

2. Error Correction

A credit card holder must report an error on an account statement within 60 days after the first statement containing the error was mailed.\textsuperscript{59} Likewise, the credit card issuing bank must investigate to either correct the error or explain to the cardholder why the statement is correct within two billing cycles and not later than 90 days after the issuing bank receives notice of the error.\textsuperscript{60} During the investigation period, the cardholder can withhold payment of the amount in question.\textsuperscript{61}

3. Dispute Resolution

If a consumer has a problem with merchandise or services that are credited to a credit card, and the consumer has made a good faith effort to resolve the problem with the merchant, the consumer has the right to withhold payment from the card issuer.\textsuperscript{62} If the card is a bank card, a travel and entertainment card, or another card not issued by the merchant, the consumer can withhold payment only if the purchase exceeds $50 and occurred in the consumer's home state or within 100 miles of the consumer's billing address.\textsuperscript{63}

4. Disclosure

Regulation Z also requires certain disclosures so that consumers can discover unauthorized transactions and errors and take appropriate action.\textsuperscript{64} Error resolution procedures must be pro-

\textsuperscript{51} See Adams et al., A Commercial Lawyer's Take on the Electronic Purse: An Analysis of Commercial Law Issues Associated with Stored-Value Cards and Electronic Money, Bus. Law., Feb., 1997, at 653, 656. However, in addition to federal regulation, "each state has enacted usury laws setting the maximum interest rate that can be charged on consumer loans." Michael A. Finler, Cyberfinance: Regulating Banking on the Internet, 17 CASE W. RES. L. REV. 81, 94 (1996).


\textsuperscript{53} See generally 12 C.F.R. § 226 (1997).


\textsuperscript{55} See 12 C.F.R. § 226 (1997).

\textsuperscript{56} "The liability of a cardholder for unauthorized use of a credit card shall not exceed the lesser of $50 or the amount of money, property, or services obtained by the unauthorized use before notification to the card issuer [as described in this regulation]." 12 C.F.R. § 226.12 (1997).

\textsuperscript{57} See Amster, supra note 20.

\textsuperscript{58} See id.

\textsuperscript{59} See 12 C.F.R. § 226.13(b)(1997).

\textsuperscript{60} See id. § 226.13(c).

\textsuperscript{61} See id. § 226.13(d).

\textsuperscript{62} See id. § 226.12(c).

\textsuperscript{63} See id.

\textsuperscript{64} See id. § 226.5a.
vided to cardholders when they first receive their cards and on an annual basis thereafter. 65 However, such disclosures may now be provided electronically. 66

D. Financial System Supervision

Because credit-based systems do not involve traditional banking functions, financial system regulations do not apply. Also, because credit-based systems are simply a means of transporting data related to a credit card transaction over the Internet, these systems do not involve money transmission. Therefore, providers of these services are not subject to the current or proposed requirements of the Bank Secrecy Act. 67

E. Data Protection and Privacy

Both users and providers need to be concerned about the use and protection of the credit card data that credit-based systems collect. In merchant-initiated systems, the information is available in an unencrypted form at both the merchant and the payment provider. 68 In purchaser-initiated systems, the information is available only at the payment provider. 69 During the past several years, there have been multiple instances where hackers have stolen thousands of credit card numbers from merchants and service providers operating on the Internet. 70

Many merchants use an Internet service provider as a "host" of their storefronts. 71 If hosts are used with a merchant-initiated system, then an additional party—a hosting service—has access to the credit card information. 72 Merchants need to select a host carefully and to get a broad indemnity from the host for improper use of financial data by the host's employees.

Today, data protection and privacy is largely governed by private contract. For example, users of Internet services get most of their data protection rights from the agreements to which they agree when they sign up to receive services.

Increasingly, governments are considering how to protect data that is sent via the Internet and what role government should take in creating these protections. The U.S. Federal Trade Commission is concerned about the privacy of data collected on the Internet. 73 Other countries have been more active in setting standards for the protection and use of data. For example, the European Union ("EU") is requiring all EU Member countries to provide legal safeguards for "personal data" about individuals that is "processed" by others. 74 Consequently, merchants and payment system providers based in the U.S. may need to comply with a variety of different data protection requirements if they are using the Internet to do business with people located in other countries. 75

II. DEBIT-BASED PAYMENT SYSTEMS

While credit-based systems currently dominate the Internet payment landscape, companies are introducing the electronic equivalents of checks, cash and debit cards for use on the Internet. 76 From a merchant's perspective, debit transactions provide advantages over credit transactions, including lower fees and limited risk of a "charge-back." 77 From a consumer's perspective, debit

65 See 12 C.F.R. § 226.5a.
68 One of the most serious threats to credit card data protection are merchant employees who are either careless or bent on sabotage. See Warding Off the Cyberspace Invaders: Internet Crime is Rising, but There are ways to Reduce the Threat, Bus. Wc., March 13, 1995, at 92.
69 See id.
70 In 1994, Kevin Mitnick stole 20,000 credit card account numbers from the databases of Netcom On-Line Communications Services, Inc. See Tsutomo Shimomura and John Markoff, TakeDown 145 (1995). In August 1997, Carlos Salgado, Jr. pleaded guilty to trying to sell 100,000 credit card account numbers that he took from the servers of an Internet service provider and several on-line merchants. See Computer Whiz Pleads Guilty in Credit Fraud, SAN FRANCISCO CHRON., Aug. 26, 1997, at A14.
71 The Internet storefront concept is rapidly expanding into the possibility of full-blown "cybermalls." See Jackson supra note 3.
72 See Harding, supra note 38.
73 See D'ALIELO, supra note 44, at 4.
76 See Adams, supra note 51, at 662.
transactions allow payments to be made on the Internet in cases where merchants have been unwilling to accept credit cards.\textsuperscript{79} For example, utilities and other service providers now allow consumers to pay their bills on-line using debit-based transactions.\textsuperscript{79} Moreover, merchants can provide low-value goods such as games, news articles or music, over the Internet and charge consumers a small charge per use.\textsuperscript{80}

A. Introduction to Debit-Based Systems

The debit-based systems are designed to permit holders of bank accounts to transfer money from their accounts over the Internet. For example, debit-based systems allow an Internet purchaser to send instructions to its bank to make payments from its checking account to the merchant's account.\textsuperscript{81} Unlike digital currency, which is discussed in Part III, the debit-based systems must receive on-line authorization from a central database before a payment can be made. In other words, funds used in debit-based payments never leave the banking system while digital currency can pass among buyers and sellers independent of banks.\textsuperscript{82} Debit-based systems generally process transactions through traditional bank payment systems, such as the automated clearing house ("ACH") or the automated teller machine ("ATM") networks; a record of each transaction is kept by a central database in addition to any records maintained by the payor.\textsuperscript{83} Typically, merchants pay the provider of the debit-based system a fee, which includes the cost of processing the payment through the ACH or ATM network. These fees probably will be $0.30 or less per transaction, subject to certain monthly minimums.

The Internet is being used in different ways to transfer funds between bank accounts. The following are the principal types of debit-based systems that are either under development or already available.

1. Electronic checks

When using electronic checks, a purchaser sends his bank account number and the routing number of his bank to a merchant.\textsuperscript{84} The merchant transmits the information over the Internet to the electronic check service provider, who submits to the ACH a debit against the purchaser's account with an offsetting credit to the merchant's bank account.\textsuperscript{85} If the purchaser uses a browser to send the information, then the merchant will be able to view the purchaser's bank account information before sending the information for settlement. Whereas, if a purchaser uses wallet software to send the information, the merchant will not be able to view the purchaser's bank account information, which is only decrypted by the electronic check service provider.\textsuperscript{86}

2. Internet debit cards

Using the Internet equivalent of an ATM card, a purchaser sends the merchant account information that is shared on the ATM card together with a personal identification number ("PIN").\textsuperscript{87} The merchant then transmits the information over the Internet to the debit service provider, who sends the ATN network a debit against the purchaser's account with an offsetting credit to the merchant's bank account.\textsuperscript{88} As with electronic checks, if the purchaser uses a browser to send the information, then the merchant will be able to view the purchaser's ATM information before sending the information for settlement. Likewise, if a purchaser uses wallet software to send the information, the merchant will not be able to view

\textsuperscript{79} See Alan S. Kay, Screen Shots. Rigs Home Banking. The Wash. Post, June 6, 1997 at 82. NUI's "Rapid Pay" system is an example of such a service. See generally NUI Home Page (visited Nov. 4, 1997) <http://www.nui.com/rapidpay.html>.

\textsuperscript{78} It should be noted that credit card issuers are trying to make it easier for merchants to accept their payment cards on the Internet. Minimum transaction amounts are being removed and, with the availability of SET, discount fees may be reduced.

\textsuperscript{80} See Joshua B. Konvisser, Coins, Notes, and Bits: The Case for Legal Tender on the Internet, 10 HARV. J.L. & TECH 321, 328 (1997).

\textsuperscript{81} See Adams, supra note 51, at 660.

\textsuperscript{82} This ignores the fact that issuers of digital currency are likely to keep the money they collect in a reserve bank. However, the issuers can never associate the funds in the reserve with any particular holder of digital currency. See Sharon Powers Sivertsen, Legal and Regulatory Issues in Stored Value Card Technologies, ELECT. BANKING L. AND COM., May, 1996, at 4-5.

\textsuperscript{83} See id.

\textsuperscript{84} See Adams, supra note 51, at 662-63.

\textsuperscript{85} Id.

\textsuperscript{86} See id. at 661-62. See also Weisman, supra note 15.

\textsuperscript{87} See Adams, supra note 51, at 662-63.

\textsuperscript{88} Id.
the purchaser's bank account information, which is only decrypted by the debit service provider.90

3. On-line stored value systems

On-line stored value systems resemble stored value cards, such as a prepaid telephone card, except that they work on the Internet. These systems require a purchaser to load value into his wallet software before making a payment on the Internet.91 Money is transferred or "loaded" into the wallet using either a credit card, the ACH, or an ATM network, as described above. Transferred funds are held in a bank account maintained by the service provider on the purchaser's behalf.92 To make a payment, the purchaser uses the wallet to send encrypted payment information to the merchant, who then passes it to the service provider for settlement. The service provider debits the purchaser's account maintained by the provider and credits a similar account maintained for the merchant.93 The CyberCoin® service provided by CyberCash, Inc. is an example of this type of system.94 The CyberCoin® service is designed for small-value purchases of goods that can be delivered on the Internet, such as stock quotes, news articles and on-line games.95

B. Consumer Protection and Loss Allocation

Federal Reserve Board Regulation E provides consumers with their main legal protections in using debit-based Internet payment systems.96 Regulation E is broad in scope and applies to any payment system that allows consumers to use a card or other "access device" to initiate a transfer of money to or from a consumer account.97 The term "access device" includes not only ATM and other debit cards but also PINs, telephone transfer and bill payment codes and other means that may be used by a consumer to initiate an electronic fund transfer to or from a consumer account.98 Although it was designed to cover electronic transactions such as ATM transfers, direct deposits and automatic payments using the ACH, transfers through point-of-sale terminals and telephone bill paying, Regulation E has new relevance in the area of electronic commerce. The Federal Reserve has said that "computer network payment products" that involve on-line access to a consumer account in a financial institution are fully subject to Regulation E.99 In 1996, the Federal Reserve proposed several amendments to Regulation E, including new rules for different types of "stored value systems," and the Federal Reserve also has suggested that these new rules might also apply to "network payment products."100

Regulation E provides consumers with the following protections: requiring disclosure of the terms and conditions of a transfer service, requiring receipts and periodic account statements, limiting consumer liability for unauthorized transfers, prescribing error resolution procedures and restricting the unsolicited issuance of access devices.101

1. Liability Limitations

Perhaps the most important feature of Regulation E is its limit on consumer losses from unauthorized transactions.102 Unlike a credit card, a consumer's liability for unauthorized electronic funds transfers is limited to $50 only if the consumer reports the loss within two business days of learning of the loss or theft of the access device.103 If the consumer fails to notify the financial institution within the prescribed time, the...
consumer is liable for up to $500. If an unauthorized transfer is reflected in a periodic statement, a consumer must report it within 60 days of the financial institution’s transmittal of the statement to avoid liability for unauthorized transfers made after the 60-day period.

Generally, a merchant who accepts an unauthorized debit payment does not have to return any money to the consumer who suffered the loss from an unauthorized transfer. Consequently, consumers and financial institutions both share the losses from unauthorized electronic transfers.

These liability limitations apply for all types of debit-based Internet payment systems. However, the proposed amendments would exempt on-line stored value debit systems with a maximum stored value of $100 from Regulation E, including the liability limitations. For example, the CyberCoin® service currently limits the amount of money that can be loaded into a wallet to $80, thus would be exempt from Regulation E under the proposed amendment.

2. Error Resolution

Regulation E requires that financial institutions follow certain procedures in investigating errors related to electronic fund transfers. The following constitutes an error: an unauthorized electronic fund transfer; an incorrect electronic fund transfer to or from the consumer’s account; the omission of an electronic fund transfer from a periodic statement; or, a computational/bookkeeping error made by the financial institution relating to an electronic fund transfer or the consumer’s request for documentation, additional information, or clarification concerning an electronic fund transfer.

When a notice of an error is received by a financial institution, the institution, in which to investigate the alleged error and determine whether an error has occurred, has 10 business days. It must then report to the consumer the results of its investigation within 3 business days. If an error occurred, then it must correct it within 1 business day. If the financial institution is unable to complete its investigation within 10 business days, the institution may take up to 45 business days after receipt of notice of error to complete its investigation provided the institution re-credits the consumer’s account in the amount of the alleged error within 10 business days of receipt of the error notice. In addition, the institution must notify the consumer within 2 business days of the account re-crediting and afford the consumer full use of the funds at issue. It must then report to the consumer the results of its investigation within 3 business days. If it is determined that an error has occurred, it must correct the error within 1 business day of the determination.

The scope of an investigation into an alleged error depends on the nature of the error. In practice, if the error involves a transfer to or from a third party with whom the financial institution has no agreement, then the financial institution may limit its investigation to its own records. If, however, there is an agreement between the institution and the third party, and the transfer in issue is one that is covered by the agreement, then the institution must contact the third party to the extent necessary to verify the transaction data regarding the erroneous transfer.

For the electronic check services and the Internet debit card services, the Regulation E investigation obligations would lie with the bank where the consumer has his account. Merchants and non-bank Internet payment service providers generally would have no obligations with respect to these investigations because neither merchants nor non-bank payment providers are considered financial institutions for purposes of Regulation E. In other words, they are not providing the consumer with an account; they are only providing transport of transaction data. However, the provider of an on-line stored value service may have investigation obligations even if the provider is not a traditional financial institution because the provider will be deemed to be providing an “account.”

---

103 See id. § 205.6(b)(2).
104 See id. § 205.6(b)(3).
105 See 61 Fed. Reg. at 19,705.
107 See id. § 205.11(a)(1).
108 See id. § 205.11(c)(1).
109 See id.
110 See id.
111 See id. § 205.11(c)(2) (1997).
112 See id. § 205.11(c)(2)(ii).
113 See id. § 205.11(c)(2)(iv).
114 See id.
116 See id.
3. Disclosure

When a consumer receives an access device and periodic statements disclosing transaction activity, Regulation E also requires initial disclosure of the consumer’s rights and obligations.117 In addition, the consumer must receive an annual notice regarding error resolution procedures.118 Generally, the financial institution providing the consumer with an account is responsible for these disclosures.119 Although Regulation E currently requires that these disclosures must be provided in writing, the proposed amendments would permit the disclosures to be delivered electronically.120

Because a non-bank provider of an on-line stored value service may be deemed to be providing a consumer with an account, these non-bank providers may be subject to Regulation E’s disclosure obligations.121 The proposed amendments would exempt providers of on-line stored value systems from the periodic statement requirement if an account balance and transaction history is available at the consumer’s request.122

C. Financial System Supervision

Unlike the consumer protection issues discussed above, the following issues related to financial system supervision are mainly of importance to providers of payment services, which must design their systems to comply with these requirements.

1. Money Laundering

For providers of payment services (including non-bank payment providers), the requirements of the anti-money laundering statute known as the Bank Secrecy Act (“BSA”)123 may be applicable. Under the BSA, financial institutions are required to (i) report and retain records of transactions in currency of more than $10,000124 (ii) maintain records of funds transfers, such as wire transfers, of $3,000 or more,125 and (iii) report and retain records regarding “suspicious transactions” and “known or suspected criminal violations.”126 While Internet payment service providers are not likely to be receiving or dispersing large amounts of cash, they may be facilitating the transmittal of funds in amounts of $3,000 or more. Consequently, banks that offer Internet payment services must comply with these requirements. However, the regulations also impose obligations on “non-bank financial institutions.”127 Specifically, non-bank financial institutions are required to keep a record of the name and address of the transmitting party, the amount of the transmittal and the execution date of the transmittal, together with certain other information, with respect to each transmittal of funds exceeding $3,000.128 An exclusion is provided if both the transmitting party and the recipient are U.S. banks.129

While the term “non-bank financial institution” has been aimed at licensed money transmitters and issuers of at least $150,000-a-month in traveler’s checks and money orders,130 the U.S. Congress in 1994 directed the Financial Crimes Enforcement Network (“FinCEN”), which administers the BSA regulations, to expand the coverage of the BSA to include firms that sell money orders and transmit funds.131 FinCEN has proposed amending the definition of financial institution to include “money services businesses”132 and to require that money transmitters register with FinCEN and report certain transactions in amounts under $10,000.133 While the definition of “money services businesses” would include providers of Internet payment services, the proposed additional reporting and record-keeping

---

117  See 12 C.F.R. § 205.7(b) (6).
118  See id. § 205.8(b).
119  See id. § 205.7(a).
120  See id. § 205.4(a); see Electronic Fund Transfers, 61 Fed. Reg. 19,696 (to be codified at 12 C.F.R. § 205(c)).
122  See id. at 19,702.
124  See 31 CFR § 103.22(a)(1).
125  See id. § 103.33(c)(1).
126  See id. § 103.21(a).
127  See 31 C.F.R. § 103.33(f).
128  See id.
129  See id. § 103.33(f)(6)(1)(A).
130  See id. § 103.11(n)(4); see id. § 103.33(f).
131  See 140 CONG. REC. H6642-01, H6692 (1994).
133  See id. at 27,909.
requirements would not apply to “advanced electronic payment systems,” such as Internet payment systems.\(^{134}\)

Under the proposed amendments, payment providers would be required to register with FinCEN and maintain a current list of their agents for examination, on request, by any appropriate law enforcement agency.\(^{135}\) Each payment provider would be required to register annually by supplying to FinCEN such information as the names and addresses of its directors, officers and controlling owners and estimates of its business volume for the coming year.\(^{136}\)

Bank providers of debit-based payment services need to comply with the existing funds transfer reporting requirements.\(^{137}\) It may be that Internet payments will not reach the $3,000 level, at least not in the foreseeable future. Non-bank payment providers will have to follow the course of the proposed amendments to the BSA regulations to anticipate whether they will have to register with FinCEN and whether additional reporting or record-keeping will be required with respect to smaller value transactions.\(^{138}\)

2. Federal Deposit Insurance

Since funds remain in a purchaser’s bank account until the payee makes a claim, electronic check and Internet debit card systems funds used in these systems would appear to qualify for federal deposit insurance.\(^{139}\) The FDIC has determined that funds held by providers of on-line stored value systems may be covered by federal deposit insurance if the funds are held in a bank in a segregated fashion or in connection with a specific transaction.\(^{140}\)

3. State Money Transmitter Laws

Under state money transmitter laws, non-bank firms that provide financial instruments such as traveler’s checks, are subject to registration and other requirements.\(^{141}\) Generally, non-bank providers of electronic check systems are not subject to state money transmitter laws because they do not hold money on behalf of others.\(^{142}\) However, providers of on-line stored value systems may be subject to the registration requirements of state money transmitter laws because the provider, through control of balance information, maintains authority over each transaction.\(^{143}\)

D. Data Protection and Privacy

Users and providers of debit-based systems should have the same concerns with security of financial information as they do with credit-based systems.\(^{144}\) In some implementations of electronic check systems, the bank account information is available in an unencrypted form at both the merchant and the payment provider level.\(^{145}\) However, in most debit-based systems (including Internet debit cards and on-line stored value systems), the information will be available only at the

\(^{134}\) See id. at 27,890.31.

\(^{135}\) See id. at 27,890.

\(^{136}\) See id. at 27,891.

\(^{137}\) 31 C.F.R. § 103.21(a)(1); see id. 103.22(a)(1).


\(^{140}\) See id. at 40,493.

\(^{141}\) See id. at 40,493.

\(^{142}\) See ARIZ. REV. STAT. ANN. § 6-1202 (West Supp. 1995); COLO. REV. STAT. ANN. § 12-52-104 (1996); DEL. CODE ANN. TIT. 5 § 2303 (1993); GA CODE ANN. § 71-241 (1993); IDAHO CODE § 26-2903 (1997); IOWA CODE ANN. § 533B.1 (West 1993); N.Y. BANKING LAW § 641 (1982); OHIO REV. CODE ANN. § 1315.02 (Anderson 1996); TENN. CODE ANN. § 45-7-202 (1993); VA CODE ANN. § 6.1-371 (Michie 1993); see also Adams, supra note 51, at 675.

\(^{143}\) See OHIO REV. CODE ANN. § 1315.02 (Anderson 1996).

\(^{144}\) See Adams, supra note 51, at 675.


\(^{146}\) See id. at 973-74; (discussing security of financial transactions in electronic commerce); see also A. Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & COMM. 395, 457 (1996) (analyzing the problem of double-spending with digital currency).
payment provider level.\textsuperscript{146} Government authorities that have been active regarding data protection and privacy, such as the U.S. Federal Trade Commission and the EU likely will be more concerned with the collection and protection of bank account information in debit-based systems than they are with the collection and protection of credit card information.\textsuperscript{147}

III. DIGITAL CURRENCY

With few counterparts in the physical world, digital currency is the least familiar type of Internet payment system. Similar in operation to stored value “smart cards” such as the Mondex card, digital currency has been described as “a foreign currency in that it has value and can be exchanged back and forth with U.S. dollars” and “requires clearing or settlement.”\textsuperscript{148} Although not yet widely used, digital currency is ideal for small-value purchases of goods that can be delivered on the Internet, such as stock quotes, news articles and on-line games.\textsuperscript{149}

In order to obtain digital currency for shopping on the Internet, a purchaser converts funds from a bank account or credit card into a electronic token that can be used to make purchases on the Internet.\textsuperscript{150} The token is encrypted data that is recognized as valid by software as it changes hands. On the Internet, these tokens can be freely exchanged without any authorization from a central database or any record of a transaction being made by anyone other than the parties to the transaction.\textsuperscript{151} Purchasers pay a small fee to the issuer of the digital currency. There are several different implementations, but they function similarly as a store of value or medium of exchange.\textsuperscript{152} The best example of digital currency is ecash\textsuperscript{TM}, which has been developed by Digicash b.v.\textsuperscript{153}

A. Consumer Protection and Loss Allocation

Since Federal Reserve Board Regulation E does not apply to digital currency, users of digital currency bear the full risk of loss for holding and accepting digital currency.\textsuperscript{154} From a consumer’s perspective, the risk of using digital currency will likely be limited. A consumer will probably hold only small amounts of value (probably less than $100) in digital currency so that theft of tokens or corruption of files containing the tokens will be the equivalent of losing some cash from a wallet. From a merchant’s perspective, the risk of accepting digital currency will likely be greater. A successful merchant will need to be willing to accept large amounts of digital currency, even though individual transactions may have a small value. Of course, issuers of digital currency must rely on technological impediments to counterfeiting in order to avoid losing money when fake tokens are redeemed for cash.\textsuperscript{155}

B. Financial System Supervision

1. Money Laundering

Both bank and non-bank issuers of digital currency face the same issues as described above in connection with the debit-based systems. In particular, non-bank issuers will have to follow the course of the proposed amendments to the BSA regulations to anticipate whether they will have to register with FinCEN and whether additional reporting or record-keeping will be required with respect to smaller value transactions.\textsuperscript{156}

2. Federal Deposit Insurance

Although an issuer of digital currency may hold the money it collects when issuing digital currency

\textsuperscript{146} See Froomkin, supra note 145, at 457.
\textsuperscript{147} See generally Ellen d’Alielo, supra note 75, at 2-3.
\textsuperscript{148} See Weisman, supra note 15.
\textsuperscript{149} See id.
\textsuperscript{150} See Adams, supra note 51, at 660.
\textsuperscript{151} See Adams, supra note 51, at 660-61.
\textsuperscript{152} See Adams, supra note 51, at 660 (noting digital coins are stored on the user’s computer until the user decides to make a transaction).
\textsuperscript{154} See Electronic Fund Transfers, 61 Fed. Reg. at 19,701 (to be codified at 12 C.F.R. § 205.16). In its proposed amendments regarding stored value systems, the Federal Reserve indicated that off-line unaccountable systems, such as digital currency, are not covered by Regulation E.
\textsuperscript{155} See Froomkin, supra note 145, at 460. (explaining how “blinded coins” make it either impossible or at least very risky for people to copy their digital cash and spending it twice)
\textsuperscript{156} See Electronic Fund Transfers, 61 Fed. Reg. at 19,699 (to be codified at 12 C.F.R. § 205.6) (proposing that Regulation E will be construed broadly to include non-bank financial institutions).
in a bank, the issuer cannot identify the specific purpose of the transaction with any particular certainty as is required by the Federal Deposit Insurance Corporation for coverage to be extended.  Therefore, federal deposit insurance generally does not cover digital currency.  

3. Monetary Policy Implications

The Federal Reserve will likely seek to address the growth in use of Internet-based payment systems and the effect of this growth on reliable economic forecasting. In testimony before the Senate Banking Subcommittee on Financial Institutions and Regulatory Relief on July 23, 1997, Federal Reserve Chairman Alan Greenspan reiterated that the “growth rates of monetary and credit aggregates have become less reliable as guides for monetary policy as a result of rapid change in our financial system.” Although the measure of the monetary aggregate M2 has, in recent years fluctuated widely, making it a less predictable benchmark for Federal Reserve projection of price stability, M2 has “shown some signs of reestablishing a stable pattern.”

Recognizing the increased use of Internet-based alternative forms of currency includes the concern that such economic activity will not be reflected in the value of the monetary aggregates. Thus, as occurred with the volatility of M2 during the early 1990’s, the Federal Open Market Committee (“FOMC”), the monetary policy setting arm of the Fed, may choose to put less weight on such monetary quantities in the charting the course of monetary policy. However, the Fed has stopped short of attributing this form of Internet payment growth to unforeseen changes in aggregate velocity (growth). Other analysts have been more forthcoming in speculating that the growth in use of Internet-based alternative forms of currency will likely pose problems for traditional economic forecasting.

C. Data Protection and Privacy

One of the most important features of digital currency is the level of privacy it provides. Merchants accepting digital currency will not need to receive any financial account information from payors. The only transaction records will be maintained by the parties exchanging digital currency. The only instance in which a financial institution would make a record of digital currency transactions is when digital currency is issued and when it is redeemed for cash in the physical world.

V. CONCLUSION

Buyers and sellers have an increasing variety of ...
methods to make payments over the Internet. However, in evaluating the merits and legal pitfalls of each system, it is important to remember that developing Internet payment systems use different payment instruments and have distinct system designs. Because of these differences, generalizations about the legal rules applicable to Internet payments are, at present, difficult to make. Before using any of these payment instruments, both consumers and merchants should consider the different sets of legal issues relating the particular type of payment system.

In general, Internet payments are not the unregulated novelty as is commonly believed. Instead, the challenge will be to adapt and expand existing laws, regulations and private contract rules to adequately cover the new medium of the Internet.