Electronic Payment Systems

Money, the primary subject of payment obligations, has a long history, an understanding of which informs the design of reliable electronic payment systems. Dating from hundreds of years B.C. the successful forms of money traditionally have two major functions: (1) **storehouse of value** and (2) **medium of exchange**. Money was once considered a storehouse of value because gold or silver coins had intrinsic value from their precious metal content. Today, few circulating coins are struck from precious metal and few paper currencies are backed by government promise to redeem them for gold or silver. This means that today, money serves as a storehouse of value only so long as the public has confidence in it. Public confidence is also essential to money’s function as a medium of exchange. Money must be widely available so that most people can use it. Money must also be widely acceptable: most people must be willingly to take it in payment for services, intangibles, goods or land.

The experience with various competing currencies in early U.S. history was negative. During Colonial and post-Revolutionary times, paper notes were issued by governments (England, colonies, states, U.S. federal), by private banks and even by other private parties. Some were backed by agricultural products, such as tobacco, meaning the currency could be redeemed (exchanged) for something of tangible value. However, the proliferation of these currencies caused inflation; many were not universally accepted for payment. The Constitutional framers reacted to a proliferation of currencies before the Revolution and during the time of the Articles of Confederation. They envisioned a single predominant currency so Congress was granted the power to coin and regulate money while that power was prohibited to the states. The states have since had the power to charter (license) banks. Currency was issued by both federally chartered banks and by state chartered banks until the taxes levied on non-federal notes diminished their use. Public confidence in money is enhanced when control is concentrated in a trusted government entity like the Federal Reserve.

**Insert Federal Reserve Screen Capture about here**

**Background: Contemporary Use of Electronic Payment Systems**

Electronic payments are hardly new. The first international wire transfer of funds occurred soon after the trans-Atlantic telegraph cable was laid in the 1880s, linking the U.S. with the U.K. The lives of few people today remain untouched by electronic
payments. The most frequent experiences are cash withdrawals from bank accounts or credit card accounts using automated teller machines (ATMs). Most credit card charges use electronic account verification and transaction processing. Indeed, the physical handling of credit card carbon impressions is nearly an extinct practice, although it resurfaces occasionally when electronic networks become temporarily inoperative. Most retail merchants offer point of sale (POS) transaction processing for debit and ATM cards using electronic networks similar to credit card networks.

Electronic payments systems are less visible, but no less important, in other areas. Consider the growing use of electronic payment systems in transportation: toll tag use at turnpikes, bridges and tunnels or charging gasoline with electronic token-readers at the pump. Even people who do not use “plastic” are affected by electronic processing of payments at the wholesale level. Nearly all inter-bank transactions between the buyer’s bank and the seller’s bank are processed electronically including the total fund transfers clearing all paper checks, direct deposits, and clearance of credit card or debit transactions by ATM or POS. Electronic payment systems can be viewed broadly to include preconditions to payment such as metering, bill calculating and invoicing.

The electronic metering and recording of customer transactions facilitates billing of telephone use, long-distance, wireless airtime, pay-per-view deliveries or on-line subscription services (ISP, Lexis/Nexis, WestLaw). Electronic bill payment and presentment (EBPP) to customers or to their automated payment services may also trigger electronic payments. Many transactions use analog or digital electronic means to transmit billing and payment information, such as use of the telephone (voice), fax (documents) or e-mail (electronic records) to communicate credit card account numbers and expiration dates to authorize payments, to identify the payor or to transfer bank draft payment using automated clearing house (ACH) facilities. Electronic bill presentment is the first step to performance of payment obligations. It may occur using email, web banking or through some third party electronic bill payment service.

<table>
<thead>
<tr>
<th>Controversy over New Money: Network Effects and Payment Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>The obstacles to innovations in electronic payments are similar to the challenges of introducing a new currency. The first barrier is switching costs. Before a payment innovation will succeed, people must believe the new system will be as convenient to use</td>
</tr>
</tbody>
</table>
as their existing money and certainly no more costly. A new currency may not be as stable as the old one. The Euro sustained considerable losses after its initial introduction. Some Europeans are reluctant to use stored value cards because they find their traditional currency works just fine. They find no compelling reasons to switch because fees are charged to use stored value cards. Of course, some consumers may pay for convenience. As bank tellers become less convenient, consumers may learn to tolerate ATM fees charged by both their own banks and by the ATM owners.

The second barrier is network economics. **Network effects** are economies of scale derived from standardization and universal acceptance. Success of payment innovations seems unlikely until critical mass is achieved. Consider the ubiquitous fax machine. It was nearly worthless until all fax machines used the same communications protocol and only then did most offices install them. As the fax network expanded, the value of the fax technology expanded. The same holds true for money and payment systems. As more consumers and merchants learn to trust particular currencies ($) or forms of payment (checks, credit cards), they become the standard forms for payment.

The implication of network economics for innovative payment systems is that critical mass must be achieved. This means that enough customer subscribers, participating merchants and infrastructure must come on line to facilitate frequent and reliable use. **Critical mass** is the essence of network effects, many systems must achieve very wide acceptance before they will be financially successful. Of course, not all markets are controlled by network effects to the same extent as are communications, payments and computer compatibility. Indeed, the measure of success for many tangible products is the achievement of small but profitable market shares. Network economics is discussed further as it impacts the antitrust laws in Chapter 19.

This section discusses the existing legal framework for electronic payment mechanisms as well as the technical and legal challenges to successful development of alternative electronic payment mechanisms. First, there is an introduction to the retail electronic transfer of payments involving both credit and debit transactions under federal law. Next, wholesale electronic funds transfer under Federal Reserve regulations, the federal Electronic Funds Transfer Act and UCC Article 4A are examined. Finally,
emerging electronic payment systems are reviewed in light of the key, enduring legal and practical characteristics of successful payment systems. These principles are projected onto proposed systems to predict the obstacles and opportunities for reliable electronic payment innovations.

**Retail Electronic Funds Transfer: Credit Cards**

When consumers directly use electronic funds transfer (EFT), these are retail transactions that can occur in two modes. First, credit card transfers are debt transactions, essentially advances made from a line of credit established between the consumer and the credit card issuer. Credit EFT transactions are based on “push technology” because a series of payment orders direct banks to make payments through the system to the ultimate payee. Second, debit transfers are deducted directly from assets held by a financial institution or from an existing deposit account with a bank. Like traditional paper-based checks and drafts, debit EFT are based on “pull technology” because they order or request payment through the system from the payor bank.

Credit cards were first developed in the 1950s. They proliferated in the 1960s as many banks issued cards indiscriminately and without careful screening for creditworthiness of prospective cardholders. After many issuing banks sustained significant losses, Congress passed the Consumer Credit Protection Act in 1970, as part of the Truth in Lending Act. The Federal Reserve is authorized to implement the Act and has done so with the strong consumer disclosure protections of Regulation Z.

Credit card transactions are also regulated by three major types of contracts: (1) between merchants and their banks to process credit cards accepted as payment, (2) between consumers and their banks who issue credit cards and (3) all participants are bound by the transaction clearing rules of the sponsoring credit card association (e.g., Visa, MasterCard, Discover, American Express). This are closed systems in several respects. The parties’ rights and duties are defined by system rules regulating acceptance of payments, processing of transactions, and the honor or dishonor of the ultimate transfer of funds. Also the transmission of transaction information is often sent via secure networks. However, consumers become vulnerable as they transmit credit card account information via the Internet. Security concerns will require the use of encryption or other protective means. For example, the SSL (secure socket layer) communications
technology is in wide use, essentially an encryption of account information during transmission.

The revenue that supports the credit card system is derived from various fees. First, a percentage of gross credit card sales are “charged-back” against the merchant accepting credit cards, called a “discount.” Effectively, this is a percentage of gross sales fee the merchant must pay (1%-5%) on the amount received in payment for the consumers’ use of credit. Second, consumers pay interest on unpaid balances, typically between 10%-24%. Third, some cardholders even pay initiation and/or annual fees.

Credit card issuers profit from these fees and this allows them to give consumers another big incentive to use credit cards: the rather considerable advantage of float. Those consumers who can time their credit card transactions and payments optimally actually borrow the amount of the purchase, interest free, for up to 50 or 60 days if they have no outstanding unpaid balances. Float has been a double-edge sword for many years impacting both the credit and debit sectors of the banking industry. The float causes many banks to lose profitable opportunities, yet some banks find ways to take financial advantage of float. Float is the result of slow and inefficient transmittal of instruments and documents as well as less than fully automated recordkeeping. Today, the elimination of float is a primary incentive driving advances in electronic payment systems.

**Regulation Z** imposes considerable consumer protection obligations on card issuers. In turn, card association rules shift many of these risks to merchants. Cards may be sent to consumers only upon consumer requests or as a renewal. A cardholder becomes liable for charges only after the issued card is accepted, either by signature, by use or by authorizing another person’s use. Increasingly, acceptance is accomplished when consumers call to activate their new cards they receive. Periodic statements of account and notices of the card issuer’s error resolution process must be sent to cardholders. Cardholders must attempt to settle disputes that arise over a transaction (e.g., warranty breach) directly with the merchant. Regulation Z gives the consumer a bargaining advantage in this: payments to the merchant can be suspended until the dispute is resolved. Regulation Z limits this right to contest charges over $50, and only those made within the cardholder’s state or within 100 miles of the cardholder’s home. Some credit card issuers currently waive these restrictions. Without this extension of
consumer protection, consumers charging purchases in distant transactions using the
Internet, phone or mail-order would not have this dispute bargaining advantage.

Cardholder liability is limited to $50 for any unauthorized charges made before the issuer is notified that the card was lost or stolen. Merchants who do not inspect the card they accept may not contest the cardholder’s claim that a particular charge is unauthorized. Card association rules shift most of this risk to merchants who must verify the identity of the cardholder. The most common verification methods include a comparison of signatures, although other methods are available, such as a comparison of the cardholder’s photograph on the card or other ID, verification using a PIN (personal identifying number) or perhaps some biometric method (fingerprint, retinal scan). Merchants accepting cards via mail, telephone or the Internet seem particularly vulnerable to credit card fraud. Increasingly, credit card issuers insure these risks in an effort to make Internet credit card use more secure and safe for consumers. Clearly, the relatively high credit card interest rates payable on unpaid balances also defray the expenses of credit card fraud and subsidize losses on delinquent accounts of uncreditworthy cardholders. These consumer protections are unequaled for any other payment method, electronic or otherwise. For this reason, Regulation Z probably accounts for the overwhelming dominance of credit card payments in retail transactions consummated by phone, mail or over the Internet. In other words, in the Internet space, “credit card is king” of electronic payments by dollar volume.

**Retail Electronic Funds Transfer: Debit Cards**

The other predominant mode for consumer electronic funds transfer is the debit EFT transaction. Since the 1970s, financial institutions have offered electronic access to retail customer deposit accounts or other assets through customer use of debit cards at ATMs or POS devices. Debit EFT also includes computer or telephone transfers, regular direct deposits like paychecks or social security benefits and direct withdrawals like periodic bill payments and, more recently, Internet bill payment services. Congress passed the Electronic Funds Transfer Act (EFTA) in 1978 authorizing the Federal Reserve to implement the Act, which it has done with Regulation E. Regulation E requires financial institutions to issue an **access device** when EFT debit services are used. Various security methods serve as components of an access device. Usually redundant
controls are best. Consider the security involved in using a debit card to withdraw cash from an ATM. The actual card must be used, a secret PIN must be entered, photographs are taken and the amount of the withdrawals is often limited so an account cannot be quickly depleted. Now consider the authentication process for bill payment using a home computer. This process might include a written pre-authorization for such transactions, an on-screen notice detailing each transaction, identification using a PIN and a paper receipt for reconciliation of records. The EFTA and Regulation E cover only the bank to consumer portion of these transactions. The wholesale, interbank transfer of consumer transactions is discussed below.

**Regulation E** is less consumer protective than Regulation Z because it places greater responsibility on consumers. For example, consumers who completely fail to notify the bank of a lost or stolen debit card could conceivably suffer unlimited losses. The $50 limit applies only if notice is given within 2 days after the consumer learns of the loss. The limit rises to $500 if notice is given after 2 days but by 60 days.

Increasingly, debit cards are branded as credit cards to broaden their acceptance beyond ATMs and POS devices to include certain merchants. As of this writing, some credit card companies are not enforcing the higher loss limits for these cards. Such lenient policies could change as consumers become reliant on them. Debit cards may not be issued or activated unless requested by the consumer and some employers now refuse to offer paper paychecks pressuring employees to authorize direct deposits.

Regulation E has no provision similar to the right under Regulation Z to withhold payments during the consumer’s dispute with the merchant for breach of contract. Debit transactions offer more disciplined spending management to financially responsible consumers because consumers have difficulty spending more than is available as deposited assets. Nevertheless, users of credit EFT methods have stronger regulatory protections under Federal Reserve Regulation Z than do users of debit EFT methods under Regulation E.

Regulation E gives consumers a right to stop payment similar to the one under commercial paper law. For example, a preauthorized EFT may be prevented, before it is actually executed, such as the regular payment of a utility bill. Regulation Z requires that banks investigate and document errors and consumers must be given documentation of all
EFT transactions actually completed. Disclosures of consumer rights under the EFTA are also required. In June 2000, The Federal Reserve proposed revisions to Regulation E to expand disclosures required for ATM fees and to allow recurring EFT from a consumer account when authorized in a signed writing or “similarly authenticated.” If the proposal is promulgated, this could permit use of some electronic or biometric means of authenticating regular EFT transactions.

**Wholesale Funds Transfers**

Before the 1989 introduction of UCC Article 4A, the only guidance for wire transfer of commercial payments among business parties was industry practice. Since then, the widespread adoption of UCC Article 4A has codified many of these practices to achieve a balance of the risks. A typical wholesale B2B payment occurs when a commercial customer pays its suppliers. This wholesale transfer of funds totals several trillion dollars each business day. These EFTs are typically made in large amounts, at high speed and at low cost using reliable electronic technologies. UCC Article 4A is technology neutral; it governs wholesale funds transfers whether transmitted by various electronic means or by traditional means such as U.S. mail.

Much of the money transferred to or from banks by consumers or other customers are eventually transferred between banks. Federal Reserve Regulation J applies essentially similar rules to the EFT between financial institutions routed through Fedwire using their regional Federal Reserve branches as conduits. Although the consumer-initiated credit or debit EFTs discussed above are excluded from UCC Article 4A, this law was prescient because its objectives and methods anticipated the problems with electronic payments arising in contemporary eCommerce. A more detailed example of a wholesale EFT transaction helps identify the parties and provides a better understanding of their major functions and the steps typically involved.

**Wholesale EFT Transaction Illustration**

Assume that East Corp. owes $45,350 for a truckload of widgets it purchased from InterWidgCo. East typically pays its bills from an account with All-National Bank. InterWidgCo. has an account with First State Bank. An EFT commences when an authorized person in East Co.’s accounts payable office uses a computer to issue a **payment order** directing All-National Bank to transmit a second payment order to First
State Bank. The All-National Bank payment order specifies that $45,350 currently held in East Corp.’s account will be transferred to First State Bank and the amount should immediately credited to InterWidgCo.’s account. When First State Bank accepts the second payment order, it notifies InterWidgCo. that the $45,350 has become available. Settlement of these payment orders usually occurs later when accounting entries are made netting all the transactions between the two banks, perhaps by the close of that business day.

In the above example and under UCC Article 4A, both East Corp. and All National Bank are senders of payment orders. Each order, in turn, is triggered by its predecessor. East Corp. is the originator. First State Bank is the receiving bank and InterWidgCo. is the beneficiary of the payment orders. If these two banks have not had regular, frequent transfer activity between them, it could be necessary to use one or more intermediary banks to act as conduits to process these payment orders.

Today, most EFT payment orders are transmitted electronically through communications systems called value added networks (VAN). Significant VANs include the regional Automated Clearing Houses (ACH), the New York Clearinghouse Interbank Payments System (CHIPS) and in international commerce, through the Society for Worldwide Interbank Financial Telecommunications (SWIFT). Payment orders can also be transmitted by EDI, fax, e-mail, phone and even on paper. When an EFT transaction is processed through intermediary banks, several VANs may be involved. VANs are closed and secure information processing systems transmitting EFTs only among members or as intermediaries for other banks or other parties.

UCC Article 4A requires that security procedures be established to authenticate transactions, verify the parties’ identities and detect errors. These concerns are similar to the problems addressed by electronic signatures discussed in Chapter 12. UCC Article 4A encourages banks to develop, regularly use and impose security procedures on customers, so long as they are commercially reasonable. Security procedures can be expected to evolve and improve over time. Examples include the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures or similar security devices.

The overriding incentive of EFT is to reduce the cost of individual verification of
payment orders, making EFT more efficient. When commercially reasonable security procedures are in place but an unauthorized payment order is processed, the loss allocation rules of Article 4A and the parties’ contract usually shift this risk to the customer. UCC Article 4A helps settle disputes concerning potentially costly errors, such as, mistaken beneficiaries or amounts, improper notices, fraudulent payment orders, and even bank failures. EFTs are typically large dollar amounts and their transactions costs are low. UCC Article 4A helps the transmitting and receiving banks to carefully design EFT procedures for themselves and their commercial customers with a view to minimizing the risk of costly errors and the opportunity for fraud.

**Future Prospects for Electronic Payment Systems**

Many experimental consumer electronic payment systems have been announced. The accompanying promotional fanfare has attracted dot.com venture capital and investor attention. However, most of these systems have eventually failed and none has yet achieved widespread success. Nevertheless, electronic payment systems may experience the greatest near to medium term growth in peer-to-peer (P2P) payments systems like “PayPal”, smart card use, electronic customer loyalty point systems, escrow services, electronic bill presentment and electronic access/manipulation of account records at banks and vendors. All these systems rely on computerized, electronic telecommunications to do one or more of the following: authorize or order payments, verify customer identity and availability of account status, documentation and record-keeping.

Paypal P2P system: [http://www.paypal.com](http://www.paypal.com)

Some day, secure electronic packets of value may actually transfer electronic currency without the assistance of trusted third party intermediaries (e.g., banks). However, third parties will remain involved with all forms of payment until electronic payment innovations are much more reliable and become highly resistant to tampering, legal and commonplace. eCommerce will likely rely on credit card usage for at least part of most consumer transactions in the near to medium term. An estimated 95% of Internet commerce payments in year 2000 involved credit cards and many electronic payment innovations depend on credit cards.¹

As with most other Cyberlaw concerns, it may be necessary to return to “basic

principles” underlying our existing law and financial institutions. A clearer understanding of the function of these institutions can then be used to project how such legal protections should be configured in eCommerce. Then, it can be determined whether existing law can adapt. If not, society can consider new legislation that is technology neutral, will still accommodate existing payment methods and then will foster the development of new payment methods.

The barriers to widespread use of electronic payment innovations are considerable. Uncertainties about the safety and security of payment innovations may slow acceptance by the public and businesses. The Federal Reserve is reluctant to surrender its control over the money supply and banks are not eager to relinquish their existing control over payments. However, the economic incentives to reduce the transactions costs of payment performances are substantial. Consider these estimated cost (in year 2000) of an in-person, bank transaction with a human teller is $1.07, an ATM transaction is $0.27 while a smart card transaction (discussed below) may cost less than one cent. The combined costs of billing consumers and their payments by check are estimated at $0.85 per transaction. As discussed in Chapter 17, there are significant incentives to innovate in electronic payment systems now that business methods are clearly patentable. Indeed, by the year 2000, the U.S. PTO had issued nearly 100 patents covering electronic payment systems. As payment laws are modernized in the future to facilitate innovation, many more patent applications for electronic payment systems can be expected.

Adapting Payment Law and Business Practices to eCommerce

The law of electronic payments is developing slowly. Before the Internet’s full potential can be unleashed, the constraints of law and business practice must be accommodated. A central constraint is that compliance is required with banking and payment laws. First, state laws require the licensing of banks. Banks have a near oligopoly control over the deposit and payment order business. Electronic payment products have been proposed by non-banks. If non-banks accept customer deposits or

---


3 *Id.*
their payment products are linked to a bank account, this may violate state banking laws. Non-banks may engage in the business of transmitting money (e.g., Western Union, GE Credit, money orders) including the movement, distribution and clearing of payments. However, such non-banks must also be licensed under most states’ money transmitter laws. Second, Regulation E may apply to electronic payments, such as the stored value systems discussed below. This would trigger the Regulation E consumer protections discussed above. Third, the Stamp Payments Act of 1862 makes it a criminal felony to circulate coins, tokens or obligations under $1 if they are intended to circulate as money. Unless repealed, this old law could severely constrain the development of micro-payments, point systems and the electronic coin purses. Fourth, the deposit insurance system is designed to protect depositors from bank failures. It can be expected that some firms will seek to remain outside the extensive regulations of the FDIC. However, customers of some other firms may still seek the safety of deposit insurance.

Innovation in the design of electronic payment schemes must also account for business practice and economic incentives. The lessons learned from the major characteristics of money and from the evolving payment schemes should be addressed. As innovations in electronic payments are analyzed, consider the following factors:

- Confidence in money is gained when its value is linked or it can be converted into something of value, such as an acceptable denomination of a respected currency ($, £, ¥) or another liquid asset with reliable value (gold).
- Electronic payment forms should be as convenient as cash, that is, readily transferable, capable of convenient exchange in scalable denominations, easily stored and transmitted or received to and from various locations.
- There must be security and accuracy in transactions.
- There must be reliable means to authenticate electronic money as genuine, not counterfeit or forgery.
- Anonymity for the purchaser is a contentious issue. Some users may seek an audit trail of all prior transactions, including the identity of payors, payees and intermediaries. This capability is now possible with checks, wire transfers, POS or credit card transactions. Law enforcement prefers traceable payments for evidence of criminal activity such as the money laundering discussed in chapter 7. Paper
currency has serial numbers and can be marked while contemporary coins are low value making them impractical for large transactions. By contrast, many other users prefer to maintain transaction anonymity. Some privacy advocates suspect that comprehensive transaction records weaken personal freedoms and become a tool for a repressive government.

- Few payment schemes are practical without the participation of trusted and reliable third party intermediaries. Third parties, like banks, provide useful services such as experience, transmission of orders, account information or documents, useful relations with correspondents, provide security and safekeeping and they can connect the payment scheme to reliable sources of value.

- New forms of money created outside the traditional framework of regulatory oversight may weaken control over the economy. Alternative forms of money and payment schemes processed outside the banking system threaten the power of the Federal Reserve and other financial regulators to control the money supply, to maintain the solvency of financial institutions and maintain the integrity of deposit insurance (FDIC).

The involvement of third parties seems indispensable for the success of electronic payment innovations. These third parties would usually include banks, financial institutions, credit card issuers and VANs. The emerging electronic payment innovators might also find additional third parties useful, including lenders, Federal Reserve, FDIC, clearing houses and escrow agents. Aside from the network effect problems of scale economies, the success of electronic payment innovations must find the right mix of third party involvement and hit the market at the right time. Consider the potential range of involvement of such third parties: (1) investment, ownership and operation of the electronic payment system, (2) research, development, standards setting and system design, (3) issuance of electronic value to consumers and financial liability for the electronic value, (4) resale agent for other issuers of electronic value, (5) recruitment of participating merchants, (6) recruitment of consumers, (7) operation of computer data and storage, (8) operation of telecommunications network infrastructure, and (9) escrow services.

**Electronically Stored Value and Smart Cards**
There have been and likely will continue to be persistent efforts to use electronic memory devices to store value for ultimate use in payments. Value stored on computers could be used in Internet transactions. Value stored on plastic cards or other portable storage devices could be used to shop in person through computer communications terminals physically held at a merchant’s premises or mounted as a PC peripheral. Stored value is really an electronic wallet, purse or piggy bank. Most such systems envision that value is added into storage by a third party who accepts traditional payment by cash, check or credit/debit card transfer and converts this to the storable electronic value. When purchases are made, precise deductions of the appropriate value are made from the storage device. Optional features of the transaction include remote authentication and authorization, documentation, transmittal of notices, private consumer behavior information accumulated, and creation of permanent records or even anonymity maintained. The precise combination of these factors as well as identity of the third party, the computer and communications infrastructure used and other architectural aspects help to distinguish the stored value experiments thus far attempted.

In the U.S. most smart card experiments have failed, e.g., 1996 Atlanta Olympics, 1998 Manhattan’s Upper West Side. Stored value cards offer consumers less protection than do credit or even debit cards under Federal Reserve Regulations Z and E (limitation on theft losses, unauthorized use). The Mondex and CyberCoin projects are repeatedly mentioned. However, American consumers seem satisfied with existing payment technologies. By contrast, smart cards are becoming popular in Europe, Japan and U.S. college campuses where the finality of cash-like transactions is appreciated and there are no realistic expectations to benefit from the float.

**Stored Value in Closed Communities: the Case of a College Campus**

An analysis of the college environment illustrates how barriers to stored value might be overcome. Most importantly, the economies of scale from network effects can occur promptly in a closed community like a college or university. The enlistment of thousands of student consumers could be accomplished by a single administrative decision. For example, university administrators can order mandatory use of smart card technologies on student ID cards (chips, magnetic strips), force standardization of communication and security protocols and select a single third party to administer the
tasks of a financial institution (bank, credit union). Remaining student reluctance can be overcome if smart cards store other data such as customer loyalty points that entitle cardholders to discounts or free merchandise. At large campuses, a single decision also immediately enlists some key merchants that conveniently reside on campus: vending machines, photocopiers, computer labs, food services, fees, event tickets, refreshments and bookstores. Local, independent, off-campus merchants may have little choice but to adopt the technology or they could risk losing significant student business. The lesson for electronic payment innovations is that critical mass must be achieved quickly because of the difficulties in overcoming consumer satisfaction with existing technologies and merchant reluctance to invest in expensive new technologies with unknown reliability.

**Federal Reserve Proposal for Electronic Check Presentment**

In year 2000, the Federal Reserve proposed a system to reduce the costs of physically moving checks between banks, Federal Reserve branches and around the country. This would involve a system for automated clearinghouse debits or **Electronic Check Presentment (ECP)**. Under this proposal, the bank that “cashes” the payees’ check, would retain the paper check and not return it for payment as done currently under UCC Articles 3 and 4. Instead, the depository bank would make and transmit an image of the check to collect from the drawee bank. If the drawer who issued the check ever requested a copy, the depository bank would electronically produce and mail an **image replacement document (IRD)** to the drawer. Federal Reserve regulations would make this IRD an equivalent of the original check for all legal and evidentiary purposes. Although a few rights and duties must be revised under Federal Reserve regulations and the UCC, the ECP proposal described here appears to be a substantial efficiency innovation for the “back office” handling of traditional paper checks and may be a step towards broader acceptance of electronic checks.

**Micro-Payments**

There is considerable Internet content that is not particularly valuable and will probably not be sold for high prices. This is not to say that healthy markets cannot develop in low priced content such as clips of sound, music or video, images, data, information and analysis. Rather, it suggests that the availability of such content is restrained until efficient and effective payment schemes are devised. As of this writing, most “low value content” is available only under one of three models: (1) for free
supposedly as part of building elusive “brand image,” (2) ostensibly free sites that
generate revenue from banner advertisements, referrals or secondary use and resale of
users private information profiles, or (3) subscription and metered pay-per-view services.
Until content providers can be paid fairly for their low value content there will be a
restrained willingness to supply more content. Website practices may not be respectful of
visitor privacy. Content providers will remain unwilling or unable to have their content
effectively bundled with other subscription services. An obvious solution to this problem
is the development of effective micro-payment technologies, small, electronic payments
made automatically and at low transactions costs.

Most existing payment schemes pose transaction costs that may consume too
large a percentage of low value transactions. Consider the difficulties with credit card
use. The transactions fees force many merchants to require minimum purchases of $10 to
$20 per charge. Some credit card issuers charge merchants up to 5% of the total sale in
fees for processing the payment. These economics make it difficult to profitably use
credit cards for sales of low value content. It is generally uneconomical to make micro-
payments to access web content on a “pay-per-view” basis. Potentially lucrative new
business models would be possible if web users could make small electronic payments,
perhaps as low as a few pennies, to receive low value website content. For example,
reliable micro-payment capabilities might replace some of the free access to Internet sites
under current usage. This would stimulate accessibility to more creative and useful web
page information, video and audio content, images and networked data if website
operators had greater incentive from more direct profits. Of course, many in the Internet
community are unreceptive to this pay-per-view model because web content has long
been freely available. However, their fears may be an overreaction. There is a compelling
analogy: video content proliferated as television viewing migrated from free advertiser
supported broadcast transmission to subscription cable television, premium channels,
video rentals and pay-per-view.

The lack of universal micro-payment capabilities relegates web commerce either
to: (1) larger transactions for goods, software or subscription services or (2) speculative
and uncertain business models. While this dilemma probably constrains very few B2B
transactions, it forces B2C and C2C transactions into a few controversial business models
such as (1) banner advertising and referrals, (2) the collection and resale of private user data and (3) brand image building. The introduction of reliable and efficient micro payments technologies arguably would release a flood of content, reducing reliance on models that are contingent on revenues from advertising or private data profiling. At this writing, the most promising models permitting micro-payments are subscription services, e-malls and e-wallets. Although some form of digital coin might be more effective, failures of the Millicent and CyberCoin experiments due to insufficient critical mass probably reflected a user population that was not ready to pay for content they still believed should remain free.

Electronic Payment Epilogue

As of this writing, at least four broad types of experimental electronic payment systems are underway. First, digital cash requires the involvement of an intermediary (flooz.com, InternetCash Corp., DigiCash Inc.). The intermediary takes in money from registered consumers who establish a credit balance with initial payment by cash, check or credit card. Payments are then dispensed for Internet purchases made from registered vendors. Second, are digital wallets. These also require consumers and vendors to register with an intermediary (Yahoo, AOL’s Quick Checkout, Microsoft’s Passport). The intermediary’s software holds the consumer’s credit card number(s) and shipping address facilitating quicker online transaction processing. In a variation of this type of system, the vendor assigns a different credit card number for each new transaction so that the vendor never learns the consumer’s actual credit card number enhancing security. Third, there are systems that more closely resemble frequent flyer points, bonus coupons or “green stamps.” These are typically issued by point-granting intermediaries (Beenz.com, E-Centives, MyPoints.com). Both consumers and vendors must register and points are earned for providing personal information or viewing ads. Finally, escrow agents are trusted third parties who hold the consumer’s payment for the vendor’s benefit until the consumer notifies the escrow agent that the goods actually arrived and conform to the vendor’s description. Escrow payments must be released to the vendor when the escrow terms are satisfied. Escrow has long been used to protect both parties in various types of transactions, notably sales of real estate.

Despite all the publicity surrounding electronic payment experiments, the most
successful systems are largely extensions of existing systems, illustrating two important points. First, consumers’ and commercial parties’ acceptance of new payment systems will depend on the proven security and reliability of those systems. Second, payment system performance depends on trusted third parties, commercial banks and other financial intermediaries, which will likely control the handling of most payment processes. e-Commerce must rely on credit cards, checks and drafts, and EFT until there is widespread acceptance of reliable electronic currency. Indeed, Federal Reserve Chairman Alan Greenspan has predicted, “Electronic money is likely to spread only gradually and play a much smaller role in our economy than private currency did historically.”