Preface

This handbook provides an overview of the major current electronic payment systems over the Internet and comments on the future of these systems. This is an important topic because electronic commerce is projected to grow to $1 trillion by year 2010. Rapid growth of the Internet and the World Wide Web are the major factors fueling the growth of electronic commerce. The Internet and the Web provide an infrastructure for business activities around the clock and around the globe. However, one of the main obstacles to this growth is the lack of secure electronic payment systems.

If electronic commerce over the Internet is to succeed, macro and micro electronic payment systems on the Internet must be developed and become secure and efficient enough to remove the public’s concern that transactions over the Internet is not secure. An understanding of the current state of the art on electronic payment systems is important for businesses planning to get into electronic commerce.

Many people have contributed to the handbook. Special thanks go to Chesney Wong and Patrick Hung. Both are technical staff of the Cyberspace Center. Dr. Kamalakar Karlapalem, Assistant Professor at the Department of Computer Science in HKUST, has provided valuable comments on the SmartFlow Internet Payment System project described in this handbook for which we are grateful. This handbook can be viewed and downloaded from our website http://www.cyber.ust.hk/publications.html

I would also like to acknowledge the Hong Kong Government Industry Department for funding the Cyberspace Center. Our objective is to help Hong Kong industries make more effective use of the Internet to enhance their competitiveness in the world market. This and other handbooks we have published are part of our effort in attaining that goal. Please visit our web site to learn about some of our other activities.

Samuel Chanson
Director
Cyberspace Center
http://www.cyber.ust.hk
1. INTRODUCTION

Electronic payment systems are central to on-line business process as companies look for ways to serve customers faster and at lower cost. Emerging innovations in the payment for goods and services in electronic commerce promise to offer a wide range of new business opportunities.

Electronic payment systems and e-commerce are highly linked given that on-line consumers must pay for products and services. Clearly, payment is an integral part of the mercantile process and prompt payment is crucial. If the claims and debits of the various participants (consumers, companies and banks) are not balanced because of payment delay, then the entire business chain is disrupted. Hence an important aspect of e-commerce is prompt and secure payment, clearing, and settlement of credit or debit claims.

The current state of on-line electronic payments is in many ways reminiscent of the medieval ages. The merchants of Asia and Europe faced a similar problem while trying to unlock the commercial potential of the expanding marketplace. Those ancient traders faced a number of obstacles (e.g., conflicting local laws and customs regarding commercial practices and incompatible and nonconvertible currencies) that restricted trade. To circumvent some of these problems, traders invented various forms of payment instruments. The merchants also developed commercial law surrounding the use of these instruments that proved to be one of the turning points in the history of trade and commerce. We are on the verge of a similar sort of development today, but one that is unlikely to take anywhere near the centuries it took for the traditional payment system to evolve.

Everyone agrees that the payment and settlement process is a potential bottleneck in the fast-moving electronic commerce environment if we rely on conventional payment methods such as cash, checks, bank drafts, or bills of exchange. Electronic replicas of these conventional instruments are not well suited for the speed required in e-commerce purchase processing. For instance, payments of small denominations (micropayments) must be made and accepted by vendors in real time for snippets of information. Conventional instruments are too slow for micropayments and the high transaction costs involved in processing them add greatly to the overhead. Therefore new methods of payment are needed to meet the emerging demands of e-commerce. These neo-payment instruments must be secure, have a low processing cost, and be accepted widely as global currency tender.
2. BATTLE OF CREDIT CARDS

Although many individual Web sites have been set up to take credit card orders online, the majority of banks and merchants have stayed away from participating in electronic commerce until a secure credit card infrastructure, managed by one of the major credit card issuers, such as MasterCard, or VISA, was in place.

Old rivals, MasterCard and VISA, who together serve about 700 million credit card holders worldwide, teamed up with some technology heavyweights, and each came up with separate protocols for conducting secure credit card transactions over the Internet.

MasterCard teamed up with IBM and Netscape to create a system called SEPP (Secure Encryption Payment Protocol) which was based on Netscape's SSL (Secure Sockets Layer) protocol, while VISA worked with Microsoft on a system called STT (Secure Transaction Technology).

The chance of a single standard for secure credit card transactions looked slim, until MasterCard and VISA, pressured by their member banks, agreed on SET (Secure Electronic Transactions) as a common standard for electronic commerce.

SET imitates the existing credit card payment methods and addresses the following requirements, imposed by the credit card companies, and their member banks:

- Provide confidentiality of payment and ordering information
- Ensure integrity for all transmitted data
- Provide authentication that a cardholder is a legitimate user of an account
- Provide authentication that a merchant is a legitimate seller of a product
- Facilitate and encourage interoperability across software and network providers, without a preference for any hardware and software platform

Some industry insiders consider the amount of cryptography used in the SET standards a security overkill. While this can increase cardholders’ confidence, it also adds to the complexity and processing overhead. SET describes a way of securing data in transit, but does not provide end-to-end security.
The major credit card issuers are:

- **American Express - $162 billion**
  - American Express is a publicly held, global travel and financial services company that provides, among other products and services, charge and credit cards.
  - American Express's main source of revenue are the annual fees it charges the cardholders and the discount rate it charges merchants.
  - Data mining is American Express's great strength which allows AmEx to customize rewards and offers based on past cardholders’ purchases.
  - American Express dominates the corporate card market.
  - American Express cardholders spend an average of $5,830 with their cards annually.
  - American Express offers its online services through the America Online, the largest private network operator.

- **MasterCard International - $512 billion**
  - MasterCard International is a worldwide payment systems company. There are 22,000 financial institutions that issue MasterCard credit cards.
  - MasterCard's U.S. cardholders spend an average of $3,200 with their cards annually.

- **VISA International - $942 billion**
  - VISA International is the largest global payment systems company, owned by over 19,000 members. This membership includes commercial and retail banks, savings and loans, and credit unions, and VISA provides the interchange systems that transfer data and funds among members.
  - VISA's cardholders spend an average of $3,200 with their cards annually.
  - Both MasterCard and VISA have wider merchant acceptance, than American Express, because they charge an average of 1.9% discount rate on MasterCard and VISA credit card transactions, whereas American Express charges a 2.5% discount rate.
  - VISA's bylaws prevents U.S. VISA credit card issuers from issuing American Express cards.
3. **ELECTRONIC PAYMENT SYSTEMS**

3.1 **Electronic Payment Systems**

Electronic payment systems are becoming central to on-line business transactions nowadays as companies look for various methods to serve customers faster and more cost effectively. Electronic commerce brings a wide range of new worldwide business opportunities. There is no doubt that electronic payment systems are becoming more and more common and will play an important role in the business world. Electronic payment always involves a payer and a payee who exchange money for goods or services. At least one financial institution like a bank will act as the issuer (used by the payer) and the acquirer (used by the payee). There are four types of electronic payment systems: i) Prepaid cash-like payment systems like Mondex, where a certain amount of money is taken from the payer before purchases are made. The money can be used for payments later. ii) Pay-now payment systems like EPS, where the payer's account is debited at the time of payment. iii) Pay-later payment systems like Visa, where the payee's bank account is credited the amount of sale before the payer actually pays. iv) Cheque-like payment system like E-checking, where a payment is done by sending electronic forms from payer to payee. Furthermore, payments can be performed on-line, involving an authorization server as the issuer or acquirer in each payment, or off-line without contacting any third party during payment. On the other hand, the term Electronic Funds Transfer (EFT) is defined as “any transfer of funds initiated through an electronic terminal, telephonic instrument, computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account.” EFT utilizes computer and telecommunication components both to supply and to transfer money or financial assets. EFT can be divided into three categories: banking and financial payments (e.g., bank-to-bank transfer), retailing payments (e.g., VISA or MasterCard) and on-line electronic commerce payments (e.g., DigiCash). Some of them are described below. Details can be obtained from the references in Section 6 and Appendix B.

3.2 **DigiCash by E-Cash**

DigiCash's E-Cash is a software-based payment system that sends electronic payments from personal computers to other workstations via a computer network, including the Internet. E-cash is based on the concept of blind signature. When an entity \( A \) wants to obtain a blind signature on a message \( m \) from an entity \( B \), \( A \) generates a blinded message \( m' \) from \( m \) and requests \( B \) to sign \( m' \) and return the blind signature on \( m \), \( \text{sign}_B(m') \), to \( A \). Only \( B \) can construct \( \text{sign}_B(x) \) given \( x \) but anyone can verify it, and \( A \) can derive the signature on \( m \) (i.e., \( \text{sign}_B(m) \)) given the blind signature on it, \( \text{sign}_B(m') \). E-Cash converts money into a digital form,
consisting of a string of numbers which can be represented in different forms. The E-Cash coins are actually very long strings of characters sent from a bank to its account-holders over a network connection (e.g. Internet) in such a way that the serial numbers are not known to the bank. The E-Cash coins, each of which has a specified value, are stored on the user’s hard disk and can be transferred in email or as data files exchanged online between payer and payee. To receive the value, the payee confirms the validity of the coins by depositing them online into an E-Cash account. This transaction will not reveal the name or address of the payer unless the payer has added this information.

3.3 **Visa-cash**

There are two main types of Visa Cash cards: Disposable and Reloadable. Disposable cards are loaded with a pre-determined value. These cards typically come in denominations of local currency. When the value of the card is used up, the card is discarded and a new card may be purchased. These cards may be dispensed from machines call Card Dispensing Machines (CDMs) which accept a variety of payment methods. Reloadable cards come without a predefined value. Cash value can be reloaded onto the card at specialized terminals and Automated Teller Machines (ATMs). When the value is used up, one can load the card again. Visa Cash is the plastic card that works like cash. A microprocessor embedded in each card stores a specific amount of money. The card holder inserts the Visa Cash card into the merchant's Visa Cash card reader. The current balance will be displayed and the cashier will enter the amount of transaction. When the user authorizes the payment transaction, the amount of purchase is automatically deducted from the card balance.

3.4 **Secure Electronic Transaction (SET)**

SET is an open standard developed by MasterCard International and Visa with IBM. It is a multi-party protocol for conducting secure bankcard payments over the Internet. Interoperability is ensured through specific protocols and message formats. SET concentrates on securely communicating credit card numbers between a payer and an acquirer gateway interfacing to the existing financial infrastructure. The information on goods/services are given to the payer. The payer then generates a payment slip using a sophisticated encryption scheme which protects the sensitive payment information, limits the encryption to selected fields to ease export approval, ties the order information, and minimizes exposures of the payer's privacy. This slip is then signed by the payer to authorize and capture the payment. The acquirer checks all signatures and the slip, verifies over the existing network the creditability of the payer and sends either a positive or negative signed acknowledgment back to the merchant and payer. SET caters to the special security needs of electronic commerce:
• Privacy of payment data and confidentiality of order information transmission.
• Authentication of a cardholder for a branded bankcard account. Cardholder account authentication is ensured by the use of digital signatures and cardholder certificates.
• Authentication of the merchant to accept credit card payments. Merchant authentication is ensured by the use of digital signatures and merchant certificates.
• Payment information integrity is ensured by the use of digital signatures.
• Special purpose certificates.
• Nonrepudiation for dispute resolution.

3.5 Mondex

The Mondex electronic cash system operates on a smart card and the microchip contains a 'purse' in which the Mondex value is held electronically. The purse is divided into five separate pockets, allowing up to five different currencies to be held on the card at any one time. The microchip also contains the Mondex security programs which protect transactions between one Mondex card and another.

Since information is in digital form, Mondex transactions can be done over a telephone line or the Internet. The microchip maintains a record of the last ten transactions and the electronic cash can be locked into the Mondex card using a code chosen by the user. Mondex’s electronic cash can be transferred directly to a retailer, merchant or other outlet to pay for goods or services, and like cash, Mondex enables transactions between individuals, without the need for banks or other third parties.

3.6 E-checking

Electronic Checking uses a digital form equivalent to the existing paper checking accounts, and works like any paper check or wire transfers, drawn against an existing checking account. Electronic Checking works with the existing bank accounts, and there is no need to change the existing account, or establish new accounts. When an Electronic Check is used to pay for a purchase, the existing electronic banking system infrastructure, Automated Clearing House (ACH), which is used for a regular paper-based checking, is used.
The major Electronic Checking issuers are:

- **CheckFree**
  - CheckFree offers an electronic bill receipt system, and makes money by leveraging the time value of money deposited in its accounts, and by charging transaction fees per electronic check.
  - CheckFree's newest offering is E-Bill, which for a fee, provides bill payment services.

- **NetCheque**
  - NetCheque is also a debit card system developed by the Information Sciences Institute and the University of Southern California.

- **NetChex**
  - NetChex offers a user-friendly and secure way of writing an electronic check by offering a PC software to its registered customers.
  - Before transmitting an electronic check over the Internet, NetChex's system security replaces the confidential bank account information with a shadow account which is used to identify the account information to the transaction processing segment of the system.
  - The Electronic check is then transmitted across the Internet to a closed system for processing.
  - Once the electronic check is received on the private system, the check is verified for authenticity and the shadow account is replaced with the actual consumer and merchant information.
  - After the transaction is completed, an e-mail is sent to the customer for confirmation.
3.7 **Smart Cards and Electronic Payment Systems**

Smart cards are debit and credit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe. Nowadays smart cards are also used as “electronic purses” that store money for people to use for everything from shopping and paying subway fares. The use of smart cards relies on the ubiquity of smart-card readers that can communicate with the chip on a smart card. In addition to reading from and writing to smart cards, these devices can also support a variety of key management methods. Some smart-card readers combine elements of a personal computer, a point-of-sale terminal, and some may be used with an Internet connection.

Electronic commerce on Internet is a popular research area, but the lack of secure payment transfer protocol was the main barrier to promote business activity on the web. Smart card technology offers a set of valuable features such as identification, security and authenticity for many different applications, especially for payment transactions. The SmartFlow Internet payment system developed in the Cyberspace Center, HKUST, as shown in figure 1 integrates the existing technology of smart card, Internet and workflow to demonstrate a new prototype for secure off-line micro-payment transaction environment. Off-line micro-payment is suitable for low value transaction and privacy protection.

![Figure 1. Architecture of SmartFlow Internet Payment System](image-url)
In the SmartFlow system, the digital money is called *SmartCash* which has a particular denomination scheme. In our prototype system, Hong Kong dollar bills of 1000, 500, 100, 50, 20 and 10 denominations are used as shown in figure 2. The system will generate SmartCash including unique identifiers (sequence of numbers) like the serial numbers on dollar bills. Furthermore, the system must also ensure privacy of the user, and enforce the security requirement that a stolen bill cannot be used by other people. The sender of information can compute a new symmetric encryption key every time to reduce the possibility of hackers breaking the encrypted code. In figure 3, there are three main components in the SmartFlow Internet payment system. One is the *Bank* which is responsible for issuing SmartCash to the *Customer*. When the Customer requests to purchase SmartCash and download it onto his smart card, the Bank will only recognize the valid smart card without checking the card holder's identity or other related information about the holder. This scheme protects the privacy of the card holder. Every valid smart card has a unique card identifier. The holder of the card is assigned a PIN (Personal Identifier Number) code which is kept on the smart card, therefore the user needs to input the PIN to operate the smart card for each use as shown in figure 2. The Bank generates SmartCash (actually its identifier) based on the specific keys for different denominations and the identifier of the smart card. The Bank will only insert the unique identifier of a bill into the relevant slot in the smart card when the card identifier matches. This means only the card with the correct identifier can receive the SmartCash generated, and no other card can get it. This hidden note value scheme provides a level of protection to the SmartCash because a third party can only view the SmartCash identifier code (serial number) even if he is able to decrypt the SmartCash. He will not be able to see that the code actually represents cash. Furthermore, only the Bank can verify whether the SmartCash is valid or not and determine its value.

![Figure 2. Payment Gateway and SmartCash](image-url)
From the Merchant's point of view, the Bank trades the SmartCash they receive by putting cash into their accounts. The Bank verifies the SmartCash identifier, and if the serial numbers are valid then the Merchant receives the money. All these interactions between Bank and Customer or Bank and Merchant are called back line interactions because they support Customer to Merchant business activities. In the front line interactions, the privacy of Customer information must be protected. It means that neither Bank nor Merchant should know the personal information of the Customer, just like in the real world. When one enters a 7-eleven convenient store to buy something, the shopper does not know (or need to know) your identity as long as you have valid money to pay for the goods or services. But the Customer trusts and knows certain information about the Merchant and Bank that provides goods or services; the related information of Merchant and Bank are released to the public in this environment. In the SmartFlow environment, there is a third party called the Merchant Authority which issues the certificates for the Merchant to certify a registered merchant and it also acts as a mediator between Customer and Merchant if problems related to the business activities. When the Customer pays a trusted Merchant for the goods or services, the SmartCash from the smart card will be retrieved and the SmartCash number will be appended with the IP address of the receiver to enforce the SmartCash will only be valid to the specific receiver. After the Merchant has received the SmartCash and verified with the Bank, the Merchant can proceed to provide follow up activities to the Customer like delivery of goods or services as shown in figure 2. The Merchant can also perform payment change if it is needed because SmartFlow supports bi-directional payment transaction between Customer and Merchant. The Merchant may directly insert the SmartCash change into the Customer's smart card if it is authorized by the Customer and Bank, or it may request the Bank to do so. Finally, the Merchant provides the Customer a receipt and stores it on the smart card for record. The smart card will keep the last n transaction records where n is determined by the card issuer.
The main concern in Internet payment is security. It is very important to ensure that the money (SmartCash) would not be stolen by a third party. For example, figure 4 shows a business activity between a Customer and a Travel Agent. If a third party, say a Hacker, is able to capture the money, then he/she may masquerade as the owner of the stolen money and reuse it for another business activity. To avoid this possibility, SmartCash is valid only if it has passed two validation checks within a time frame. Just before the SmartCash is to be transmitted from a sender to a receiver, the SmartCash needs to pass a validity check from the sender's smart card reader. The smart card reader retrieves the SmartCash from the sender's smart card, and generates a tab using the location of the receiver with a time-stamp. The time-stamp is used to calculate the time limit of a valid SmartCash on the Internet, and it means that the SmartCash is no longer valid if the time limit has expired. The SmartCash is checked again when it arrives at the receiver to see if the time has expired and if the receiver's location matches that on the SmartCash. If the SmartCash is invalid, only the bank is authorized to revoke it back to the valid...
Moreover, in figure 4, there is a covert channel which is a secret and secure channel for two parties to perform payment transaction. For example, two parties can choose the secure private network to transfer SmartCash instead of the insecure Internet. Covert channel is used to transfer confidential information without knowledge of third parties. However, the covert channel is given a finite useful lifetime as well. The lifetime of the covert channel is affected by the time and number of parties that know about the channel. As the values of these two factors increase, the security risk of the covert channel rises. When the security risk reaches some dangerous level, the parties need to change to another channel in order to maintain the low security risk.
Another significant security issue in Internet payment transaction is when the business activity involves more than two parties. Figure 5 shows an example of *Ticket Purchasing Activity*. When the Customer books an air ticket from a Travel Agent, the payment transaction is executed between these two parties. Indeed, the Travel Agent is acting as a middleman between the Customer and the *Airline Company*. There will be business interaction between the Travel Agent and the Airline Company which is hidden from the Customer. There is another security risk here if the Travel Agent compromises the business agreement between the Customer and the Airline Company. For example, the Travel Agent receives the payment from Customer and delivers a fudged air ticket to Customer. One solution to this problem is the Customer can pay a *locked* SmartCash to the Travel Agent. The Travel Agent cannot trade the *locked* SmartCash for cash until it has received the key from the Airline Company to unlock the SmartCash. The Airline Company will issue the key to the Bank only if the air ticket for the Customer is issued successfully and payment is received from the Travel Agent. This scheme will ensure the customer will get the proper service or goods.

The first version of the SmartFlow prototype system has been implemented and it is ready for demonstration at the Cyberspace Center in The Hong Kong University of Science and Technology. The *Smart Bank Card* is implemented on an ACS smart card as shown in figure 6. The card contains 1-Kbyte EEPROM memory which holds data for the application. The ACS smart card is a memory card with security control logic which is compliant with ISO 7816-3, T=0 protocol, DES and MAC capabilities. It contains the identifier of the smart card and the user password which is changeable by the user. The security control logic protects the memory on the card such that it can not be amended illegally, but it can be read when the issuer code and password are submitted. Also, different memory locations can be protected using different security control mechanism.

The system is developed on Windows Platform using ActiveX which is written in Visual Basic to build the system logic and front-end. The back-end is supported by Windows NT Server and all related data are stored and managed by MS SQL Database Server. The system is implemented using the Internet Information Server running on a Windows NT Server, and the communication channel is secured by Secure Socket Layer (SSL). Internet Explorer 4.0 is used for the browser because Active X is only supported by Internet Explorer.
3.8 Open Trading Protocol

The OTP standards enable a consistent framework for multiple forms of electronic commerce, ensuring an easy-to-use and consistent consumer purchasing experience regardless of the payment instrument or software and hardware products used. The protocol is freely available to developers and users, and builds on XML, an emerging standard for information exchange on the Internet. As a set of truly open standards, the protocol is not owned by any one company, and its development will be managed by an appropriate independent organization.

The OTP standards specify how Internet trading transactions can occur easily, safely and efficiently for all parties, independent of the method of payment. This is similar to the trading environment in the physical world. Many existing protocols such as Secure Electronic Transaction (SET), a global industry standard for secure credit card payments over the Internet, focus on making a payment. The OTP standards complement but do not replace these protocols by providing a clearly understood set of rules that cover offers for sale, agreements to purchase, payment, the transfer of goods and services, delivery, receipts for purchases, multiple methods of payment, support for problem resolution, payment brand and protocol selection. In addition to providing consumers with a consistent approach to trading on the Internet, consumers will also have records of purchases which could be used for tax purposes, making expense claims, feeding into financial management software or sending a claim back to a merchant to solve a problem.
# 4. SUMMARY OF ELECTRONIC PAYMENT SYSTEMS

<table>
<thead>
<tr>
<th>EPS</th>
<th>Type of System</th>
<th>Target Market</th>
<th>Security &amp; Privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td>CyberCash</td>
<td>Credit</td>
<td>Home banking and catalog sales, recently added small-scale nickel &amp; dime</td>
<td>Customer’s bank receives detailed info on each transaction, but customer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>transaction system</td>
<td>retains anonymity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Payment is guaranteed before any product is shipped; liable for credit card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>transaction fraud</td>
</tr>
<tr>
<td>Open Market</td>
<td>Credit</td>
<td>Can handle any kind of transaction, from pennies to thousands of dollars</td>
<td>OpenMarket keeps detailed records, but maintains customer anonymity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Merchants can choose their preferred method of payment; liable for credit card</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>transaction fraud</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Flexible system; currently developing an online business community centered around a bank</td>
</tr>
<tr>
<td>First Virtual</td>
<td>Credit</td>
<td>Ideally suited for low to moderately priced info sales</td>
<td>First Virtual keeps detailed records, but maintains customer anonymity</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Merchant is never the consumer; because the customer gets the product before</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>paying for it, however, merchant gets a delayed payment thru an automated</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>checkinghouse</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Minimal risk to the e-mail system, but is cumbersome</td>
</tr>
<tr>
<td>Checkfree</td>
<td>Credit</td>
<td>Anything practical to sell using a credit card</td>
<td>Both merchant and bank can track purchases made by consumer</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Merchant is liable for credit card transactions</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Future plans are to expand CheckFree Wallet for check and electronic cash purchases</td>
</tr>
<tr>
<td>NetCash</td>
<td>Debit</td>
<td>Mainly for info products under $100</td>
<td>Neither bank nor merchant can track</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Merchants have a choice of assuming risk &amp; accepting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Requires correct change for each</td>
</tr>
<tr>
<td>System</td>
<td>Type</td>
<td>Description</td>
<td>Risk</td>
</tr>
<tr>
<td>----------------------------</td>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>NetChex</td>
<td>Debit</td>
<td>Products &amp; Services as well as bill paying</td>
<td>Non-anonymous</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mondex</td>
<td>Debit</td>
<td>Handles both large &amp; small transactions</td>
<td>Completely anonymous</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Netscape Secure Commerce Server</td>
<td>Credit</td>
<td>Credit Card Transaction type sales</td>
<td>Merchant risk – same as credit card transaction for getting paid</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DigiCash* (Cyberbucks)</td>
<td>Debit</td>
<td>Small-scale nickel &amp; dime purchases and fund transfers</td>
<td>Neither the bank nor the merchant can track consumer purchases</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*DigiCash has filed for chapter 11 protection in November 1998 after a round of job cuts earlier in 1998 failed to keep it afloat. The closely held company was about US$4 million in debt.
Commercial uses of the Web is still so new that almost everyone is still searching for a business model that would make sense in the emerging cyber environment. For individual shoppers, electronic commerce has definite limitations and drawbacks, lacking among other things, social interaction, which can not be replicated electronically.

However, many goods and services, such as computers, Web-related products, music, etc., are prime candidates for business-to-business, and consumer-to-business electronic commerce transactions. Music is currently the most popular of all Web consumer purchases, with over 10,000 music sites and 350 music distribution sites, where the top 5 sites are selling more than 25,000 CDs a day.

There are no guarantees on how fast electronic commerce will take off or how big it will get. But companies such as IBM, AT&T, Microsoft, Netscape, and VISA, among others, are working to generate more and more interest in electronic commerce. New technologies are also being developed or would be developed that would create a secure infrastructure for electronic commerce transactions on the Internet.

Electronic commerce must offer incentives to attract cyber buyers and sellers, by offering goods and services that the customers could not get any other way. Successful Internet merchants would need to create 'virtual' communities, where like-minded individuals would 'meet', swap information, buy something, and come back again and again.

These cyber communities, such as GeoCities, are not passive TV-like experiences, dispensing news, information, and entertainment to the masses, but cyber gathering places, creating compelling reasons for people to belong to such communities. Many content providers are bankrolling these communities, because such communities are considered the most promising advertising opportunities on the Web.

The electronic payment infrastructure over the Internet is only a part of the whole Internet-based electronic commerce equation. Future global electronic payment systems would not simply replicate existing payment methods in the cyber space, but will take full advantage of the unique nature of the Internet and the Web. Such systems do not currently exist and need to be developed to accommodate not just the current transaction safety and security issues and concerns, but a host of geopolitical and legal issues that a true global payment infrastructure would need to address.

Conclusion
With the rise of the Internet, electronic commerce is also increasingly taking place using a transmission medium that is not under the control of the financial systems and is outside of known geopolitical boundaries.

Factors such as the accelerating rate of change and complexity in technology, globalization of markets, organizational factors, and increasing demographic diversity, would drive the future of electronic commerce.

Among various electronic payment systems in the short term, secured credit card transactions are positioned to become the preferred method of electronic payments. But such systems alone are not without weaknesses, since they do not address the problem of micro payments.

Issues of security and privacy need to go beyond protecting networks, to protecting and guaranteeing digital data, and SET and other technology standards are expected to increase the comfort levels of individuals and businesses in the security of transactions over the Internet.

Transaction anonymity in cyber space could create the potential for counterfeiting and a vehicle for laundering money and evading taxes, which would not escape the attention of financial regulatory organizations worldwide.

New technologies would change the current electronic payment systems and would ultimately provide privacy and security, but not anonymity, which magnifies potential risks of electronic commerce.
6. REFERENCES


3. David Chaum. Digital Signatures and Smart cards

4. DigiCash. Blue Smart card.
   http://www.digicash.com/smartcards/blue/

5. M. Froomkin. Flood Control on the information Ocean: Living with Anonymity, Digital Cash, and Distributed Database
   http://www.law.miami.edu/froomkin/articles/oceanno.htm

   http://www.ini.cmu.edu/jg40/90-742/mondex.html

   http://www.mondex.com/mondex/

   http://info.isoc.org/HMP/PAPER/181/
A. Other Electronic Payment Methods

Electronic commerce players are teaming up with banks, credit card, EDI, and software companies, to create an infrastructure that can support business over the Internet.

Major players developing Electronic Payment products and systems are:

- **AT&T**
  
  AT&T announced the most comprehensive electronic commerce service in the industry, including a turnkey solution for businesses to design, build, and maintain Web sites, transaction capabilities via AT&T SecureBuy Service, and guaranteed credit card transaction security for cyber shoppers, backed by satisfaction guarantees.

  AT&T's SecureBuy Service is based on Open Market's OM-Transact Web commerce software.

- **First Virtual Holdings**
  
  First Virtual's system does not rely on any form of cryptography, or require any special hardware or software. Customers must have an Internet e-mail, and a valid VISA or MasterCard, which is transmitted initially by phone to First Virtual. First Virtual assigns a virtual PIN to a customer, who in turn uses this virtual PIN instead of a credit card number to place an order with a merchant. First Virtual then sends an ordinary e-mail to the customer, to confirm the purchase.

  First Virtual's type of operation, where a third party processes credit card transactions, is called a 'factoring' operation, which according to VISA International guidelines is against the law.

- **IBM**
  
  IBM's CommercePoint products is among the first to utilize SET protocols to provide safe credit card transactions over the Internet.
IBM's CommercePoint includes World Commerce, a service to build and maintain merchant sites; World Distributor, a service that ties together retailers, franchisers, suppliers, and other vendors and provides purchase order processing, and catalog creation; World Purchasing, a service designed for large businesses and governments that do contractual buying and selling; Net.Commerce Payment, a suite of products for secure credit card payments; and Net.Registry, a public key registration and management service.

IBM and 15 major banks announced the creation of Integrion Financial Network, in order to put the banking institutions in the forefront of Internet-based electronic commerce, and allow the banks to control the technology for paying bills electronically. Electronic Bill payment would be Integrion's first service offering.

➤ Microsoft

- Microsoft launched Merchant Server, its electronic commerce software for the merchants, hoping to attract thousands of merchants that have been reluctant to open online storefronts due to the cost and complexity of setting up shop and the uncertainty of the online market. For less than $20,000, Merchant Server gives businesses the shrink-wrapped tools, applications, and templates they need to merchandise, process orders, and transact payments online. Microsoft's Merchant Server comply with the SET protocol.

➤ Netscape

- Netscape LivePayment extends the Netscape's development platform by providing Web sites with a point-of-sale terminal. LivePayment integrates financial transactions with Web page content, and provides a low cost solution for developing Web sites that can execute financial transactions over the Internet, using encryption technology.

➤ Open Market

- Open Market develops, markets, licenses, and supports software products that allow customers to engage in business to consumer and business to business Internet commerce. Open Market's OM-Transact software, offers business customers complete order management, online customer service, security, buyer authentication, record-keeping, flexible purchasing and payment methods, and secure transaction processing, including sales tax and shipping charges.
Oracle Corporation

To catch up with other Internet players, Oracle, the largest maker of Unix-based relational databases, announced a comprehensive electronic commerce strategy, including products and partnership alliances. Announced products included a Web Merchant Server (written entirely in Java) to allow businesses to set up a Web storefront with rich content and transaction processing capability; a Payment Server offering SET-compliant options for purchasing with credit cards, electronic cash, or electronic checks; a Security Server to issue and manage digital certificates; and a high-end electronic publishing component for publishing mail-order catalogs on the Web. The partners included Hewlett Packard, EDS, and Quark, Inc.

Trilogy Development Group Inc.

Trilogy has joined Open Market and OneWave Inc. to offer a complete package of electronic commerce products for end-to-end solutions. Trilogy would provide tools to conduct sales and marketing from Web sites, Open Market would provide software to manage transactions and provide security, and OneWave's products would integrate the other pieces and provide access to the Legacy systems.

VeriFone

VeriFone is the leading supplier of point-of-sale credit card systems, and is intent on being a major Internet transaction-system provider, by developing a bridge between the existing credit card payment networks and Netscape's Web software. In 1997, VeriFone bought EIT, the company that developed S-HTTP and formed CommerceNet.

CommerceNet is a consortium of Silicon Valley semiconductor manufacturers, software companies, financial institutions, information providers, and other businesses, aiming to develop Internet technologies that will secure commercial interaction among businesses.
B. A List of Useful EPS Reference Sites

Credit Card handlers

- VeriFone Internet Commerce
- Concord Systems
- Checkfree
- GCTech - Micro and Credit Card Payment Systems
- ICVerify - Credit Authorization Software
- American Banking Systems
- Internet Checks
- Cybercash

Electronic Payment Systems

- DigiCash
- CMU's NetBill Payment System
- ZyberCash
- NetCash at ISI, USC
- NetCash at NetBank
- NetCheque
- First Virtual
- LETSystems
- Mondex
- Netcheq
- Intell-A-Check
- Release Software
- ATS - check services
- Atomic Software
- TelPay Canada
- NetCard