Opportunities, Options, and Obstacles in Electronic Commerce

by L. Jean Camp

Columbia Institute for Tele-Information
Graduate School of Business
Columbia University
809 Uris Hall
New York, NY 10027
(212)854-4222

Opportunities, Options and Obstacles in Electronic Commerce

L. Jean Camp
Research Fellow
Department of Engineering & Public Policy
Carnegie Mellon University
Pittsburgh, PA 15213
camp+@cmu.edu

Prepared for the Columbia Institute for Tele-Information Conference on the Future of Electronic Banking

1. Introduction

Not too long ago, every currency system was based on the exchange of special items: paper, shells or metals. In electronic commerce, every system depends on the exchange of special information: passwords, challenges or account numbers. Electronic currency represents a conceptual break from currency as records with physical presence. It represents as fundamental a change as was the creation of currency with no intrinsic value.

With the advent of symbolic currency, when the objects used for exchange no longer were intrinsically valuable, an entire range of new markets was created. Similarly, no single application will be optimal for every electronic need. Letters of credit, traveler's checks, certified checks, money orders, personal checks and legal tender all evolved from the conceptual break from currency as requiring objects with intrinsic value. Multiple electronic currency types will evolve as well.

As with symbolic currency, some risks of electronic currency are clear. Others will emerge as electronic currency is adopted into daily business practice and electronic commerce expands. Several risks are already apparent: remote attacks, ease of currency duplication and the reduced time for risk assessment intrinsic to the capacity for high speed transactions. In addition, the widespread use of electronic currency generates the risk of the creation of a mutual and constant surveillance society where all actions are taken in view of employers, marketers and government.

The risks of electronic currency in other dimensions are unclear. For example, the evolution of symbolic currency and thus the banking system created an additional risk of large scale collapse. This risk was only recognized after individual banks were networked in a complex web of loans and credits. Similarly, the advent of electronic funds transfer can magnify the weaknesses of cash control systems (Fischer, 1988; Mayland, 1993). Even risk averse policies that strengthen cash control systems increase the risks of detailed information gathering, such as threatening the consumer with data surveillance (Compaine, 1988; Fenner, 1993; Chaves, 1992; Madsen, 1992).

Just as entire communities cannot be secured for the use of symbolic currency, so entire networks cannot be secured for the use of electronic currency. Therefore, electronic

currency systems must depend upon secure end points and reliable transactions within larger unsecured networks. In addition electronic commerce systems should offer consumer privacy. The solutions to security problems that have worked for paper currency do not apply to electronic commerce. Those solutions used for wire transfers and other electronic large inter-corporate transfers are not economical for consumer electronic commerce. Thus, new answers to the questions of reliability and security that fit this new computing environment are needed.

In this work I will explain the fundamental characteristics necessary for secure transactions, the options for securing servers, and the options for provision of customer privacy. I will then look at four very different Internet commerce proposals: NetBill (Sirbu, 1995), Digicash (Chaum 1992), Anonymous Credit Cards (Low, 1993) and First Virtual (First Virtual, 1995). I provide an overview of a transaction in each system and show how they differ in dimensions of reliability and privacy. While I cannot offer the definitive answers to these new questions, I will define the range of reasonable options and illustrate the strengths and weaknesses of each.

2 Reliability

Reliable transactions are the foundation of electronic commerce. A network running an unreliable protocol cannot be secure, because funds may disappear or be contested. After a network failure, with a weak protocol a system failure cannot be distinguished from an attack. These failures or attacks can be used effectively for theft.

Reliable electronic commerce requires authentication, fail-proof transactions, and controlled access. These fundamental requirements imply other technical requirements. It is widely agreed that an electronic currency system must provide divisibility, scalability in number of users, conservation of money or tamper-resistance, exchangeability or interoperability, and availability (Cross Industry Working Group, 1995; Okamoto, 1991; Neuman, 1995; Low, 1993; Brands, 1993). All of these requirements mean that the transactions themselves must have certain properties. These properties are described below.

2.1 Transactional Security

Electronic commerce transactions must be atomic, consistent, isolated and durable. Transactions with these properties are called *ACID* transactions. Distributed ACID are

robust transactions and can prevail in the face of network outages, replay attacks, failures of local hardware and errors of notoriously unreliable human users (Gray, 1993).

A transaction is *atomic* if it is all or nothing. Funds are conserved in an atomic transaction. For example, consider what happens when a customer transfers funds from a savings account to a checking account. Either the checking account is credited and the savings account is debited or neither account balance changes. There is no case where money either disappears from both accounts or is credited to both accounts. The account transaction in this case is atomic.

If a transaction is *consistent* , all relevant parties agree on critical facts of the exchange. If a customer makes a one dollar purchase then the merchant, the customer and the bank (if it is involved), all agree that the customer has one less dollar and the merchant has one more dollar.

Transactions that do not interfere with each other are *isolated.* The result of a set of overlapping transactions must be equivalent to some sequence of those transactions executed in non-concurrent serial order. If a customer makes two one dollar transactions then the two payments should not be confused. The customer should not end up being charged twice for one item nor should one single payment should not be counted twice to give the two dollar total.

When any transaction can recover to its last consistent state, it is *durable*. For example, if the customer physically drops a dollar when making a purchase that dollar does not disappear. Similarly, money that was available to a computer before it crashed should not disappear when the machine reboots.

Atomicity, consistency, durability and isolation in a transaction create the possibility for *irrefutability*. An action is irrefutable if it can be clearly proven to a third party that the action occurred. Suppose a customer wants to make a purchase from the local furniture store. The customer must pay, or promise to pay. The merchant either gets payment or proof of intent to pay in a standard purchase order or check. The customer gets a receipt from the merchant indicating that she has paid and expects the merchandise to be delivered. When it is delivered, the customer signs a receipt for the merchant indicating delivery has occurred. Each action is linked with some verification of the action so both parties have some proof in case the other party attempts fraud or fails to perform.

Electronic commerce transactions should have the ACID properties.

2.2 Reliable Delivery of Purchases

Electronic commerce is concerned with the problems in the electronic analogies of sending cash through the mail and shipping merchandise without certified delivery. The purchase of physical goods can be simplified by physical location. It is quite possible for the customer to follow the physical delivery of the item from the merchant's possession to the customer's possession. In electronic commerce the customer simply sends a payment, or promise of payment. The merchant sends the item in return. There is no delivery man with the item. The customer could claim not to have received the item after its delivery, or the merchant can claim never to have received payment.

Different degrees of atomicity address the problems of remote purchases: no atomicity, money-atomicity and goods-atomicity (Camp, 1995).

First, electronic transactions may have no atomicity. No atomicity requires mutual trust among participants. The physical equivalent is sending cash or goods in the mail to a post office box. Among electronic currency systems (See Section 5) on-line Digicash has no atomicity; meaning the merchant can claim never to have to received payment (Yee, 1994). First Virtual customers can claim not to have made a purchase or received an item. Customer or merchant fraud can be simple in systems with no atomicity.

Second, electronic transactions may have money-atomicity. The physical equivalent is sending a purchase order, meaning that the customer can prove that the merchant has been paid. However, in these systems there is no mechanism for certification of merchandise delivery. If used for remote purchase with accepted techniques for the delivery of physical goods, money-atomicity is quite adequate. But fraud can be trivial when systems with only money atomicity are used for goods with on-line delivery (ex. software).

Third, electronic transactions may have goods-atomicity. Goods-atomicity corresponds to using a certifiable payment mechanism with certified delivery in a physical transaction. Goods atomicity provides the highest reliability and reduces the opportunity for merchant fraud.

Atomicity is further complicated by the fact that traditional techniques for atomic transactions uses *rollback*.. Rollback is a technique where all steps are recorded and then inverted until the most recent consistent state is reached. For example, if a customer attempt to transfer funds into savings fails, funds withdrawn from the customer's checking account are placed back into the customer's checking account. Superficially, electronic transactions are just exchanges of bits and if the exchange can be reversed then the transaction can be made secure. Yet for Internet commerce to expand there must be some interoperability not only between forms of Internet commerce but also between Internet currency and traditional forms of money. Therefore, if the rollback period is too large a transaction that is theoretically atomic and secure is not truly atomic. During the rollback period the fraudulent party could abscond with unrecoverable cash, making the acquisition of bits meaningless.

3 Security

Secure electronic transactions require reliability. It is meaningless to call an electronic commerce system secure if that system cannot first dependably transfer funds from one entity to another. Systems that are not reliable even when intruders are absent cannot be secure. However, reliability does not assure security.

3.1 Threats

In order to understand the options for making electronic commerce secure, first understand the threats in the electronic realm. Eavesdropping, replay attacks, cryptanalysis, attacks on secure servers, disruption of transmissions and denial of service attacks are all threats to electronic commerce systems.

As in the physical world, security is never absolute. The cost of security must be balanced by the price of the loss of security. It is important when estimating the cost of these breaches in electronic commerce systems to recognize that security breaches once made can go undetected for some time. In addition, the physical difficulties and dangers that limit the attraction of repeated robberies and break-ins in the physical world do not exist in the electronic realm.

Eavesdropping is illustrated today in the theft of calling card numbers and ATM card information. Once this information has been stolen and is available in electronic form it

can be easily transferred over the network. A successful eavesdropping technique will be shared and repeated. The pay-off of eavesdropping can be reduced or eliminated by encrypting transmissions.

Replay attacks take advantage of the ease of duplication of information. Merchants can attempt to be paid twice by replaying electronic messages that verify payment. Similarly individuals can defraud legitimate users of a system by replaying authentication sequences. These problems can be solved by using authentication techniques impervious to replay attacks or by adding information in each transaction to make it unique. Authentication techniques that leak no information are called *zero-knowledge authentication techniques*. (Feige, 1987; Tygar, 1991). Random information can be added to a communication to make it impervious to replay attacks.

Cryptanalysis refers to the analysis of encrypted transmissions for the purpose of breaking an algorithm or obtaining a key. Cryptanalysis can be defeated by using secure algorithms with well-chosen keys. It is not possible to defeat cryptanalysis by using a secret algorithm. In fact, using a proprietary algorithm can be very risky, since such algorithms cannot be subject to widespread scientific review.

Attacks on secure servers are almost certain to occur. This is the electronic equivalent of a run on the banks' vault. On the positive side, the value of a successful electronic assault can be limited more easily than in the case of physical vaults. Building a truly secure server is possible, though difficult. Standard weaknesses in operating system and windowing environments can undermine the apparently secure applications running on them.

Disruption of transmission is a special case of a denial of service attack. These attacks limit the availability of your system, denying its use to you and your customers. The same threats exist in the physical realm: that someone will steal your hardware, threaten your customer or vandalize your business front making it unusable.

3.2 Basic Cryptographic Tools

Cryptography can provide authentication and security if properly implemented and integrated into a reliable electronic commerce system. There are two basic types of cryptography: public key and private key.

In *private key* cryptography the parties wishing to communicate share a key. If a message is encrypted with this private key only those possessing the private key can decrypt this message. Because encryption and decryption use the same key, private key cryptography is sometimes called *symmetric*.

There are many key exchange or key protocols which allow users to select a key. It is easiest for users to select a key if there is a central trusted server that will provide a key when requested. It is easiest for the administrators of a system if the users select a key, as key management can be quite difficult.

With *public key* cryptography, there is a set of keys: a published key and a secret key. Information encrypted with the secret key can be decrypted with the matching published key. This way, secret key encryption can be used to verify a signature, because the ability to decrypt a document with the published key proves that the owner of the secret key made the original encryption. Information encrypted with the published key can only be decrypted with the secret key. This means that information encrypted with the published key can be widely broadcast but remain unreadable to everyone except the holder(s) of the secret key. Because the possession of one key does not allow you to both encrypt and decrypt messages, public key encryption is sometimes called *asymmetric.*

One class of useful cryptographic functions is *hash functions*. With a hash function information is encrypted so that it can be used for verification but cannot be read. A common use of hash functions is maintaining password files. A machine or system can use a hash function to store passwords so that user passwords can be verified, but having the password file gives no information about a user's password. Software for cracking passwords works by randomly guessing passwords, applying a hash function and then verifying the result is in the password file. (This can be quite effective since users often use common names or dictionary words as passwords.) Many hash functions exist that will produce an unpredictable but verifiably different value for every possible input. These are called *collision-free* hash functions, and are most widely used.

For a complete discussion of the practical applications of cryptography see Schneier, 1994. (A newer, more complete version of this text will soon be available as well.)

3.3 Authentication

Authentication means proof of authorization. Authentication is based on shared information or the ability to prove unique information. With shared information it is most simple to require that one party present the information as proof of identity to another party. This means the presenting party must trust the verifier. Cryptographic techniques enable mutual authentication (Rabin, 1978; Schnorr, 1990; Feige, 1987; Rivest, 1978).

These techniques differ in the way that authentication is provided and are therefore subject to different attacks. All cryptographic authentication techniques are based to some degree on *one-way functions*. A one-way function is something that is easy to do, but hard to undo. For example, it is much easier to multiply two large numbers than it is to factor one large number. The technique in Rivest (referenced above) is in fact based on the difficulty of factoring numbers. A second common cryptographic authentication technique, Schnorr, is based on the difficulty of logarithms, while the Feige and Rabin techniques are based on the difficulty of finding square roots. These algorithms depend on the relative ease of multiplying numbers, taking a number to a power and squaring numbers, respectively.

In the case of passwords, of which PINs are a special case, the customer's ability to produce a unique number provides authentication. But since the customer gives that number to the ATM or POS terminal, this means the customer has to trust the terminal. In practical terms, this means when one ATM is badly protected or unreliable, any bank connected to the network can be harmed. This authentication procedure results in attacks such as fake ATM machines (Davies, 1981; Business Week, 1993; Johnson, 1993), thieves' programming cards with others' information (Harrison, 1994), and large losses at badly-managed machines (New York Times, 1995a; New York Times, 1995b). A similar weakness in the credit card clearing system allows disbarred merchants to use terminals belonging to dishonest merchants (Van Natta, 1995).

The problem of untrustworthy hardware can be addressed three ways: requiring secure hardware; requiring the merchants and customers to secure their own terminals; and accepting the cost of fraud in delivering low-cost items. Electronic transaction systems which require secure hardware are called off-line or smart card systems. (Smart cards are described in the next section.) Most on-line systems require customers and merchants to assure the reliability of their own hardware. Systems which simply trust the user and accept the corresponding losses are called *crypto-less* systems.

Even when all parties are honest, networks are not always reliable. Therefore, the reliability of acknowledgments should not be critical to an electronic commerce system. With some electronic transactions systems, the protocol assumes a trusted network, with reliable acknowledgments. While it is true that high level transactions protocols such as TCP can provide acknowledgments when packets are delivered, there is no acknowledgment of the contents of the packet. Thus the acknowledgments developed for reliable packet transmission are not adequate for verification for electronic commerce transactions. These acknowledgments are not secure, thus they provide only information, not authentication.

3.4 Secure Hardware

Before further considering threats to secure servers, divide electronic commerce systems into on-line systems and off-line systems. On-line systems depend on real time authorization. Off-line systems depend on secure hardware, often in the form of a smart card. Both system require cryptographic techniques for security.

Security in on-line systems depends to different degrees upon the security of trusted servers. Every commerce system uses servers trusted to some degree: servers that maintain accounts, create electronic money or authorize transfers. These servers must be both secure and highly available to the customer base.

Although the problem of secure servers is far from trivial, it is simplified by the fact that these are special purpose servers. There is no need for a trusted electronic commerce server to use the most handy tools for potential intruders: mail, ftp and telnet. Furthermore, unlike transactions theory, server security is an advanced and maturing field (Denning, 1992 ;Davies, 1981; National Computer Security Center, 1985).

Off-line systems are based on distributed secure hardware instead of a centralized trusted facility. Here you need to trust the smart card, a credit card sized device for use in a desktop machine or a public terminal. Smart cards are feasible, both in the form of additions to standard computing hardware and as stand alone smart cards, and available from many manufacturers. The quality of such hardware varies widely: specialized hardware can be tamper-proof or trivial to defeat. The existence of smart cards means that terminals must authenticate themselves to the users, as well as the users authenticating themselves to the terminals. Smart cards are active devices. This means they can refuse

attempts at reprogramming, initiate dialogues, and reject information requests. Because smart cards use trusted hardware, providing anonymity is straight forward in off-line systems.

Currently major credit card producers are considering adding smart card technology to standard credit cards to increase security (Echikson, 1994; Hansell, 1995). (The addition of secure smart card technology to standard credit cards illustrates that privacy and security are separate issues.) With smart cards, transaction authorization can be limited to a single transaction, so that traditional attacks based on obtaining credit card or calling card numbers would be fruitless. The capacity to demand verification from a terminal would mean the end of the opportunity for fake ATM terminal attacks.

Off-line devices must still communicate intermittently with a centralized server. The opportunity for attacks that affect on-line services exist during this window of connectivity. It is best to design a system so that the loss of server integrity would not be disastrous. Although all electronic commerce systems depend to some extent on secure servers, the damage done when a server is subverted varies. In some systems the subverted server could be used to electronically print untraceable money indistinguishable from valid money (Chaum, 1985; Chaum, 1992) although perhaps only in small denominations. There are systems where the subverted server could effectively only electronically print the equivalent of marked bills, because the credits could be detected as false later (Low, 1993; Sirbu, 1995). In at least one system, the failure of an authorization server would result only in claims which could be refused by the customer (First Virtual, 1995). Another approach, as seen in the facilities provided in the Web browser Netscape for secure transactions, requires that every merchants' server must be secure. Netscape requires that merchants decrypt and store a credit card number to obtain payment. Any failure of a merchant server could release a large number of credit card numbers. The danger of this is illustrated by the fact there is at least one large file of credit card numbers from Netcom currently circulating on the Internet.

Having a secure server does not guarantee that the application running on the server is itself secure, nor does it imply that the client connecting to the server is secure. The application and operating system must be complemented by the physical security of the trusted device. If a customer or merchant leaves his or her account open, authorized and connected to the server in a public cluster, then the security of the electronic commerce system is damaged despite the best design of server and application.

The hazards of accepting popular software applications as secure is illustrated by three increasingly effective attacks against the secure version of the web browser Netscape. The first attack against Netscape was simply an illustration of what was already known: any forty bit key, including Netscape's, is not safe from a determined brute force attack . The second attack was more surprising, and illustrated that the use of predictable information made it possible to obtain Netscape keys in thirty seconds or less (Markoff, 1995). The most recently reported attack identified a bug in all Netscape servers that would allow any hostile browser take over any Netscape server machine (Sandberg, 1995). (This implies that all clients need to be trustworthy.)

Secure applications for electronic commerce are a matter of both design and implementation. Furthermore, the producer of the consumer application cannot control the computing environment chosen by a customer. Therefore, as in the case of centralized trusted servers, the damage possible in the case of a subverted client application must be counter balanced by the security of the client application and its environment.

3.5 Availability

System availability can be compromised by malicious hackers, network failures or commercial espionage. To be useful and marketable, a system must be available.

Availability requires reliability, but reliability is not sufficient for availability. Availability means that any system needs to be scalable in the number of users. Of course, it is not possible to reliably scale a system that is not isolated; however, isolation alone does not guarantee scalability. (Recall that isolation, the *I* in ACID, means transactions do not interfere.) Availability and scalability are functions of the need for central processing.

Availability and scalability can be increased by migrating processing load away from the server to the customer or merchant. This is done with the current ATM network by allowing the machine at the end point to verify the PIN. In NetBill, the central servers' load is decreased by making the merchant sign using RSA and the central server uses DSS (Cox, 1995). This is a good choice, since the only disadvantage to using both protocols is that the code is somewhat more complicated. (RSA and DSS are signature algorithms. They can provide equivalent levels of security.) This migrates load because DSS

signatures require relatively few CPU cycles, but verification is computationally intensive. Conversely, RSA signatures are computationally intensive but easy to verify.

Availability for the individual merchant or customer is also a function of network availability. If a system depends on real time access, then system availability is a function of the reliability of the network as well as the number and size of messages required by the protocol.

4 Privacy

An insecure system cannot be private. A high-privacy system must be able to protect data from random or unauthorized release. Insecure information which can be involuntarily released cannot be private; privacy requires security. Conversely, privacy makes security more difficult. When the parties in a transaction can not be identified afterward, successful fraud can be easier. Reparations cannot be obtained for security holes that are detected after violations in an anonymous system, as those who have profited will be unidentifiable.

The best option in terms of privacy is to limit the collection of consumer information except as minimally necessary. This means that system designs must be closely scrutinized to determine the minimum data needed. Since some information must necessarily be compiled, the extent and uses of any compilation should be considered before entering into the electronic commerce marketplace.

4.1 Why Provide Privacy

The provision of anonymity and privacy are generally agreed upon. However, there is no consensus on the optimal choice of anonymity, psuedonymity, and traceable psuedonymity (Cross Industry Working Group, 1995; Okamoto, 1991; Neuman, 1995; Low, 1993; Brands, 1993). Yet privacy is a definite consumer concern (Ross, 1995; Longo, 1995); and the provision of privacy is a marketing as well as a moral issue (Hendricks, 1994; McLean, 1994; Hatch, 1993; Dowling, 1993).

Economic information provides information about the customer's physical and psychological health, associations and beliefs, that is appropriately known only in extreme circumstances. Given that consumers who use data repositories can easily be forced to

provide information during employment applications, consumers may be hesitant to use financial services where detailed information is compiled.

In addition to the need for consumer confidence, there are regulatory constraints on privacy. In the United States the dissemination of financial information may regulated by the Federal Trade Commission. The European Union limits dissemination of consumer data. Neither jurisdiction has a formal requirement for security or cryptography, only that no business practice include the unnecessary disclosure of information. Fundamentally, the Europeans have chosen to protect data only through policy means. The option of protecting consumer privacy only through policy and traditional database protection techniques is not as reliable as other technical options; however, it is widely accepted.

Privacy in electronic currency is not binary; there are many possibilities, from full disclosure to complete anonymity. Users can be pseudonymous, anonymous, or identified as a member of a privileged group, rather than an individual. The granularity of identification choices expands as commerce becomes increasingly electronic. Common solutions to the conflict between the need for information and the threat of data surveillance include anonymity, conditional anonymity and psuedonymity.

4.2 Anonymity and Psuedonymity

The identity of an individual is stored as just another data field in an electronic information system. Any information may be hidden or private during a transaction. When the information that is hidden is the identity of the customer, then that transaction is anonymous.

Anonymity means that the identity of a party cannot be determined during or after a transaction. Conditional anonymity means that a party cannot be determined during a transaction, but may be determined afterwards in special circumstances. True anonymity may be technically feasible in electronic commerce, but for reasons of law enforcement such anonymity may not be desirable, and will be in fact illegal for some transactions in many jurisdictions, including the United States.

Pseudonyms are aliases. Psuedonymity means that a customer can be uniquely identified for an individual transaction or attributes of a user but the user's identity can not be determined. A pseudonym may provide a billing address, a delivery address, or

verification of membership (for a discount, for example). A user may choose to have unique pseudonyms for each transaction, or to use the same pseudonym for multiple transactions, or chose a pseudonym for each merchant. Without a delivery address, or with an intermediary that hides the delivery address, a pseudonym provides no identity information.

Conditional or traceable anonymity is possible with electronic information. Traceable psuedonymity means that the chosen alias can be linked to the user's true identity. Many so-called anonymous remailers really provide traceable pseudonyms, since the records of the remailer can reveal the identity of the user of the service.

Credentials are a form of pseudonym that reveal only group membership. Unlike a pseudonym it therefore gives partial identity information. For example, a user of an AARP discount is over sixty. Unlike a constant pseudonym, it does not allow a user to be identified uniquely in sequential transactions.

4.3 Outlining the Options

As decision makers are faced with growing consumer concerns about privacy they face three basic options. The most risk averse choice is to require that consumer data be protected by both technology and policy. For those with complete faith in technology, there is the second option of relying only on technology. The third option is to rely on stated policy alone.

4.3.1 Compilation and Disclosure

In terms of policy, an institution has only the fundamental choice to gather data, or not to gather data. Using cryptographic techniques, a company may choose to collect only aggregate data (Camp, 1994). Aggregate data can provide the information for many necessary accounting and marketing functions without creating threats to privacy. Questions such as, "How many users who view our page also return later and purchase our products?" can be answered with anonymous updates if consumers have sufficient storage and processing abilities.

The decision to use off-line or on-line systems is orthogonal to the decision to provide privacy. In fact one on-line protocol, Netcheque, offers users the ability to select how much information about themselves is provided. Since off-line systems use trusted hardware, hardware is available to deter consumer fraud.

If an organization offers consumers off-line systems then the decision to provide anonymity is bound to the decision to offer debit or credit cards. It is simple to provide anonymity if the card is a debit card. Anonymous smart cards that offer consumers credit enable consumers to make charges and then lose the card before the charges were linked to the consumers account. The disadvantage to the Mondex card is that when a card is lost all the value that is stored in the card is lost as well. In that way it is very much an electronic wallet. Smart cards can be built so that card issuers and merchants would continue to obtain information about the customer, amount, items, time and location of each purchase.

Regardless of the technology chosen some data compilations will be necessary for audit and reporting purposes. Both limiting the data in the compilation and limiting disclosure of that data mitigate the privacy effects of compilations. Policies that limit disclosure or give consumers the option to limit disclosure can make consumers more comfortable about data compilations.

The policies of financial institutions on compilation and disclosure have to adjust to government decisions on the rights of individuals over their own data. Within the regulatory framework, marketing questions remain. Can customers sell their own data from company compilations? Can consumers request that data be deleted at the end of a contractual agreement?

Strong market forces push for the dissemination of data, since customer trust is lost in the long term but profits are realized in the short term. Even if only aggregate data is marketed, the privacy issue remains because of the potential for the recovery of personal information (Duncan, 1989). The level of user consent necessary for data marketing, whether implied or explicit, varies across political boundaries.

Pricing issues arise as part of the discussion of disclosure. Repositories may pay consumers for data distribution or consumers may pay for increased privacy. Consumers may agree to be on mailing list for some compensation. Consumers pay escrow agents to track and filter requests about them.

4.3.2 Escrowing Data

For data compilations where the individual is identified the data can be distributed or escrowed to minimize opportunities for disclosure. Identity can be encrypted with the keys stored in a distributed fashion (Micali, 1993; Walker. Brand); or the data can be stored in a distributed form that can be reconstructed (Shamir, 1979; Cox, 1995; Low, 1993).

This can be done using *escrowed* data. When data is escrowed the pieces are separated so that knowledge of one piece lends no information about the other (Shamir, 1979; National Institute of Standards and Technology, 1994). For example, to escrow the number 4 in the form x+y =4, x could be 2 or 2,000,000 and y correspondingly 2 or -1,999,996. Knowing either x or y gives no information about the sum but knowing both indicates the sum exactly.

Escrowing data can limit abuse by curious employees, protect against accidental or malicious release and protect against malicious alterations. If data is properly escrowed in different repositories and one repository is breached no information is revealed, no alterations made will go undetected and availability of data from other repositories is not affected (Shamir, 1979; Micali, 1993).

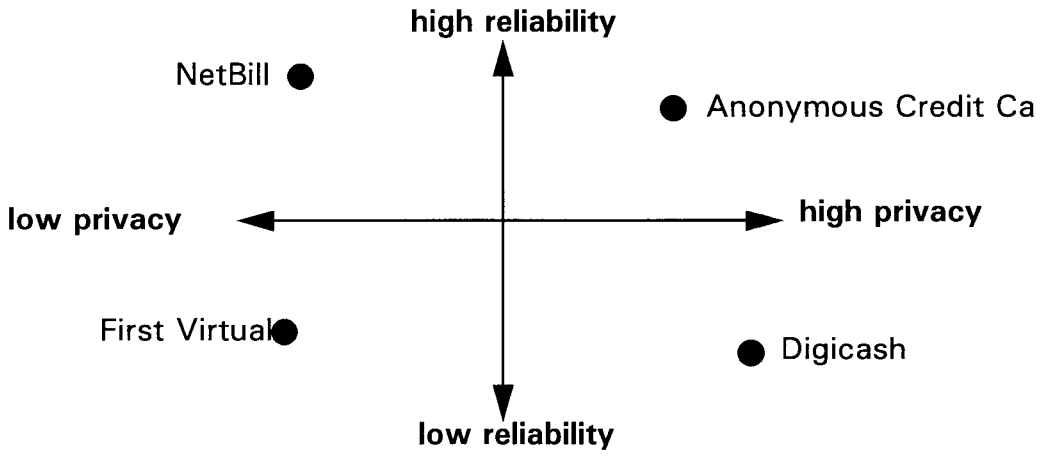
Options exist for the provision of anonymity; the virtual separation of data repositories; the real time verification of data; and the physical separation of repositories. One proposal for consumer data security requires that individuals use structurally separate institutions with their communications encrypted and routed through designated communications exchanges (Low, 1993). A second option is to have separate agencies within one organization hold information (National Institute of Standards and Technology, 1994). A third option is to separate data so that one party knows the participants while others know the content of a transaction (Sirbu, 1995). The greater the separation of data the less accessible the data. Conversely, greater separation can also mean greater security.

Technological privacy protections alone are tempting because once in place, little supervision is necessary. Yet even given the range of technological protections, policies to protect the data are necessary complements. Some of these policies need to be explicitly considered before implementation, because otherwise the policy decisions will be implicit in the implementation. These polices include limits on disclosure for repositories, consumer rights over the information in a repository and pricing of data.

5 Examples of Electronic Commerce Systems

Three basic elements have defined my discussion of electronic commerce: security, reliability and privacy. Much security must be provided at the implementation level. Reliability and privacy must be provided at the design level. To show how design decisions affect reliability, security and privacy I examine four electronic commerce systems designed so that they are compatible with the delivery of information products over the Internet. (The most dramatic deviation from standard currency, and therefore potentially the greatest opportunity, is in the on-line purchase of information goods.) The four systems are NetBill (Sirbu, 1995), Digicash (Chaum 1992), Anonymous Credit Cards (Low, 1993) and First Virtual (First Virtual, 1995).

The four systems are conceptually based on four different models of consumer commerce. Digicash is modeled on legal tender. Anonymous credit cards are modeled on standard credit cards. NetBill is based on the model of a checking account. First Virtual resembles nothing so much as mail order purchases, with the uncertainty of ordering and delivery goods without guarantee. These four systems span the range of privacy and reliability possibilities as shown below.



Reliability and Privacy of Four Electronic Commerce Systems

For each system I first describe a transaction at high level. I describe the purpose of each step in the transaction. I then offer a brief analysis of reliability and transaction-level security. I then discuss the possible effects if the secure server assumed in each system is violated. The section entitled "server security" can only address the potential cost of a server break-in and not the details of the server security as implemented. Each system has

a reference which includes a detailed technical description of each transmission which discusses fields, protocols and encryptions.

5.1 NetBill

NetBill, the Carnegie Mellon Internet billing server (Sirbu, 1995), uses an electronic ledger system, a bank which holds all money, and customers and merchants who send authorizations for transactions. NetBill was designed to sell information goods. NetBill aggregates transactions, resolves disputes, and sends account transfer instructions to the bank.

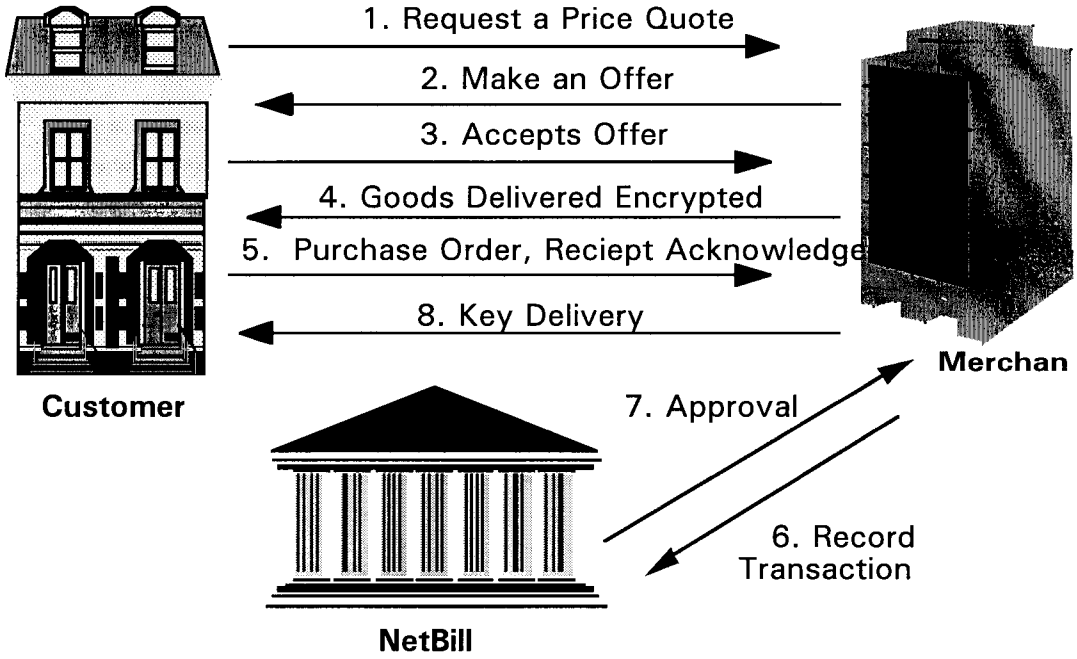
NetBill provides very little privacy. NetBill must know not only that some transaction has occurred, but also that the two state changes (debit and credit) required in the transaction are linked. This means that the customer and merchant accounts are linked during a transaction. However, NetBill is reliable and can assure that goods are delivered.

Note that the customer's having a bank account implies that NetBill knows the customer's identity: NetBill will be aware of all its customers purchases, as is a bank with a standard checking account. In a standard NetBill transaction the merchant will also know the identity of a customer; although for a fee customers can make transactions using a pseudonym that hides their identities from a merchants.

NetBill transactions are atomic. In addition to account changes being atomic, they must also be consistent. This strengthens the requirement that the customer and merchant accounts be linked by the banks for a transaction. NetBill offers fully ACID transactions.

5.1.1 A NetBill Transaction

NetBill transactions require eight steps. These steps are shown in the diagram below.



A NetBill Transaction

The diagram shows the customer and merchant negotiating a price, and coming to an agreement. In step four the information goods are delivered, but they are encrypted. This means that although the customer has the goods, the customer cannot use them. The goods are encrypted in a one-time private key chosen by the merchant. The customer then pays for the item. To get reimbursed the merchant must present to NetBill an authorization for payment, a receipt signed by the customer, a description of the goods cryptographically signed by both the merchant and the customer, and the key to the encrypted goods which is also signed by the merchant. NetBill will not transfer money to the merchant's account if all those items are not present. After NetBill has approved the transaction and agreed that the merchant's transmission was in order, then merchant sends the key to the customer. If the customer does not get the key or if the goods are not as described the customer can obtain the key or a refund, as appropriate, from NetBill.

5.1.2 Transaction Reliability and Security

If the NetBill protocol is interrupted at any time after step two it can be restarted without loss. After step two, the customer still has the option of buying the item at the offered price. After step three the merchant has a commitment to sell. After step four the merchant can repeatedly send the item. Since the item is encrypted at delivery at step four, the merchant does not need to worry about not being paid, as the key has yet to be delivered.

NetBill provides pseudonyms for consumers that can be used for a single transaction, or for each transaction with a particular merchant. Pseudonyms can be linked with authorization to specific discounts, and access control (for children, for example) can be maintained.

Notice that the customer cannot verify that the item delivered is indeed the item requested until step eight. At step four some encrypted item is delivered, but the content cannot be determined. This will undoubtedly give rise to some disputes. First Virtual solves this problem by automatically refunding money. Conversely, NetBill monitors merchant complaints instead of customer complaints. NetBill receives hash values that can verify that the item promised was the item delivered. Since NetBill receives the hash value of the item, rather than the item, NetBill cannot make detailed records of the specific items purchased by its customers. NetBill can and does keep records of the general buying patterns of its customers.

Disputes over quality of merchandise are inevitable in any type of commerce. This is less of a problem with physical information goods since I can flip through a book or paper before I purchase it. To limit merchant fraud, NetBill tracks complaints of this variety against merchants to assure that merchants are not misleading customers.

5.1.3 Implications of a Security Failure

The critical question about the security of Net Bill's server is the question of when funds are actually transferred in the bank accounts themselves. A loss of security in a NetBill server would allow NetBill to authorize bogus transactions. These may escape detection until the customer objects to the charges on his or her bank statements. If this is the case, any NetBill attacker could have up to one month to change accounts and abscond with funds. If merchants are not credited until customers approve transactions, then loss of server security would be costless. Thus, the financial security of the NetBill server depends on some policies yet undetermined. If merchants are provided with immediate access to NetBill funds, the loss of a NetBill server could be quite high.

The loss of security of a customer's NetBill account would allow the attacker to spend the NetBill customer's funds.

NetBill keeps sufficiently detailed information that in the event of fraud an audit trial would remain. This would aid both customers, merchants and NetBill in the recovery from a crash.

5.1.4 Privacy

The problem of customer location information being provided to merchants can be addressed by the use of intermediaries (Cox, 1994). Customers may also use a pseudonym; however, continued use of the same pseudonym can result in the customer's identity being part of the information connected to the pseudonym.

NetBill customers must purchase their privacy. A customer may choose to pay to have a merchant see his or her pseudonym instead of his or her identity. With the use of credentials, consumers may remain pseudonymous and still obtain discounts or rights offered only to members of select groups. This way users can keep their identities private and still provide authentication information. However, neither a customer nor a merchant can hide his or her identity from NetBill.

The only information not available to the NetBill server is the actual purchase. NetBill has only the checksum of the goods purchased.

5.2 Anonymous Credit Cards

The anonymous credit card model (Low, 1993) is similar to the current credit card model. The anonymous credit cards uses a network of banks which extend credit to individuals, and communicate through a centralized exchange to complete transactions.

Anonymous credit cards provide conditional anonymity. This means that transactions are normally private but can be traced in cases of fraud. The transfer of funds is reliable with anonymous credit cards; but there is no provision for the delivery of goods.

5.2.1 An Anonymous Credit Card Transaction

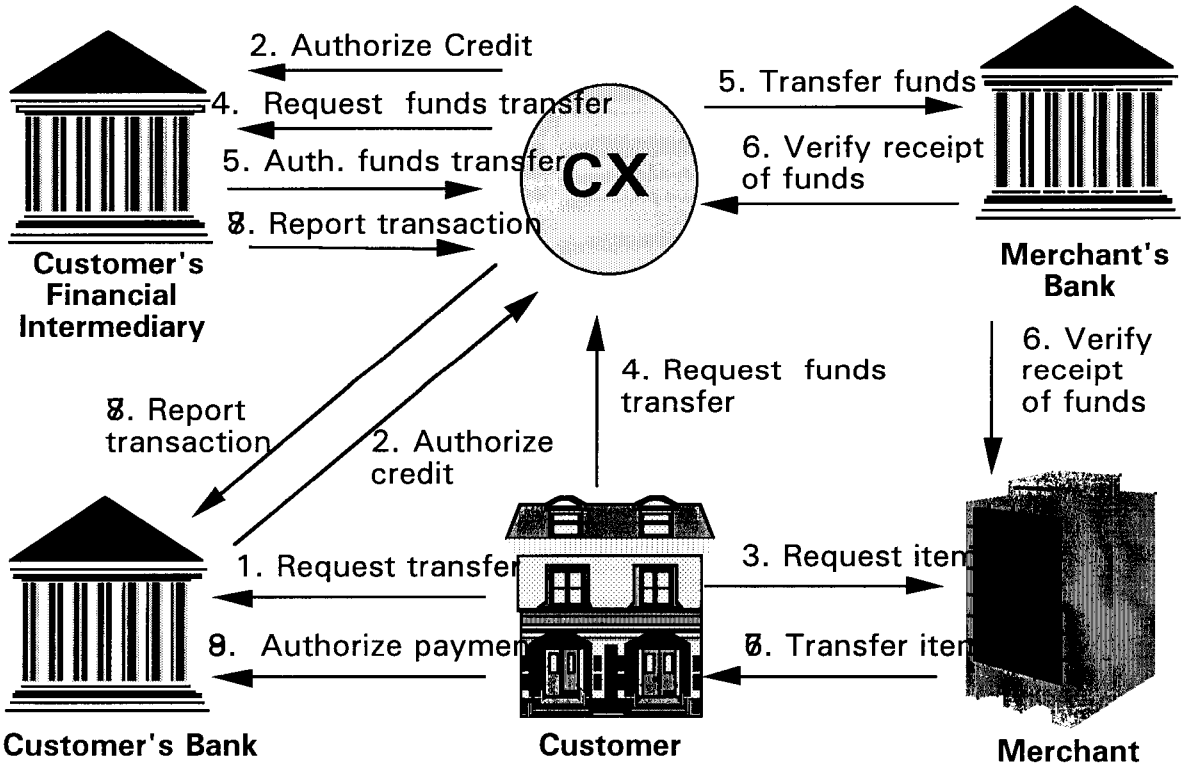
Each customer has a bank, which has an account that is linked to an anonymous account at a second bank, the customer's financial intermediary. The customer's intermediary knows that the customer's bank is credit worthy. The customer's bank must believe that the customer is credit worthy, and thus extends credit to the customer upon request. The merchant has an account at his own bank.

In a transaction a customer would browse through the merchant's wares. The customer would end the browsing transmission and begin to send a series of messages through the communications exchange to initiate a purchase. If the merchant can match the browsing to the transaction then some identity information is leaked.

Before any transaction occurs, the customer's bank knows the customer's identity. The private bank knows the customer's pseudonym and the PIN, the questions and a hash value of the answers that the person claiming the account should know. These answers are needed for authentication. The customer knows the virtual location and the commercial identity of the merchant.

The diagram below shows the transfers for a purchase to be completed in a transaction using anonymous credit cards. In the following description the customer will be presumed to be female and the merchant male for clarity of exposition.

Before making a purchase, the customer must send a request to her bank to ask for an extension of credit through her financial intermediary. The customer's bank does not need to know the identity of the financial intermediary. By requiring that messages from the customer's bank to her financial intermediary go through the communications exchange, the anonymous credit card protocol prevents the banks and the financial intermediary from conspiring to identify the customer.



An Anonymous Credit Card Transaction

When a customer chooses an item, she contacts the merchant. The merchant gives the customer his own account information. The customer then sends this account information to her financial intermediary. The financial intermediary authorizes a transfer of funds to the merchant's account and sends this authorization to the merchant's bank. The merchant's bank credits the merchant's account and notifies the merchant and the customer's financial intermediary. Last the financial intermediary debits the customer's account.

The customer is notified of this and other debits in a periodic report, much like the current credit card cycle. Note that the customer's bank cannot read the detailed transaction record, because it was previously encrypted by the customer.

5.2.2 Transaction Reliability and Security

Consider the possibility of failure at each step of the anonymous credit card protocol. At any point before step three failure means that no funds will change hands.

The customer does not know that step four was successful unless the merchant sends the requested good. If the merchant were dishonest, the merchant could force repeated payment by abruptly interrupting the transaction after step six, requiring the initiation of a new transaction. The customer would not know that the funds transfer in the first transaction was successful until step eight. The customer's financial intermediary would not know if the customer was making multiple purchases from one merchant or being defrauded. Due to the anonymity in the system the financial intermediary could not inquire. The customer's financial intermediary will not detect the failure until it is time to balance with the customer.

If the transaction fails at step six, then the merchant bank is paid but the customer is never charged. Neither the customer nor the store has an incentive to identify the misappropriation, because neither will gain when consistency is restored. This could be the most expensive failure to detect, and require much data matching. However failures of this type could be prevented with a time out mechanism, so it is not a serious problem. (A time-out mechanism would mean that the transaction would have to be completed and verified by all parties before a given time or it would be canceled.)

If transmission six arrives safely to the customer's financial intermediary, but the message to the merchant is lost, then the customer bank can verify to the merchant that the transaction succeeded. But the customer may be unable to provide that verification for many weeks. Thus, it is possible that money can disappear for the duration of the billing cycle. After the customer receives her banking statement the merchant's bank can verify that there was no success code received from the merchant. The money could then be deleted from the merchant's account and credited to the customer.

The anonymous credit card system is not goods-atomic. There is no way for the merchant to verify that the goods were indeed sent to the customer. The customer has the ability to contest credit exchanges, and can prove that she paid for the items in question. The banks and the communication exchange together can verify that money indeed changed hands from the customer to the merchant. The loss of anonymity is not required to contest a charge because the customer can communicate pseudonymously.

The merchant has some transaction identifier which does identify that the customer indeed paid. The merchant cannot prove that the item the merchant delivered was the item requested. Only the customer has access to verifiable information about the order. If the customer began the transaction with the intent to deceive, then fraud would be straight forward. Especially on information goods, or goods the consumer may want only for a short time, this could be tempting. Conversely, there is no way to prove that the merchant did not send the goods. Therefore, merchants could defraud customers by refusing to send goods.

Thus, the policy decision as to who will get a refund will create some opportunity for fraud for one party. (Given that in the current credit card system merchant fraud costs more than customer fraud, allowing the customer leeway appears to be a the risk-averse choice.)

Of course, any bank or any merchant may guess at the identity of any customer. Using the same pseudonym, or anonymous account, over time can result in a loss of anonymity as other participants update their probability distribution at each pseudonym use, eventually becoming certain of customer identity. This issue has not been addressed in the design of anonymous credit cards, but it could be solved by changing customer's accounts on a periodic basis.

The anonymous credit card system is money-atomic if merchants are not allowed access to customer funds until the consumer verifies the transaction through the billing process.

5.2.3 Implications of a Security Failure

Anonymous credit cards require more than merely an exchange of passwords for a customer to obtain funds from a financial intermediary or her own bank. The customer needs to provide a password and take part in a question and answer session to prove her identify. Thus, the loss of a customer's password or even the customer's key is not critical, and could be detected before any fraud occurs .

A customer and merchant could conspire to break bank security and siphon funds. Since the financial intermediary comes to the customer's bank only periodically, if a merchant could withdraw funds at any time, this could mean that a careful criminal could cycle funds

from an account or group of accounts for one month before the customers bank had the necessary information to detect subversion.

The loss of security for a financial intermediary could be either more or less problematic. A financial intermediary could authorize payments from many fake accounts and provide valid credit reports to customers. However, if financial intermediaries are required to settle at the end of each day or cannot maintain an overdraft with the merchant's bank, fraud detection is possible. Here issues of bank to bank clearing, daylight overdrafts and trust of other banks need to be considered.

In all cases fraud is eventually detected, and anonymous credit cards assure a trail is left to the identities of the criminals.

5.2.4 Privacy

Anonymous credit cards provide the customer with a high degree of privacy on a day to day basis. However, when the financial intermediary and the customer's bank collude customer's purchases can be traced. This reflects a reasonable compromise between the hazards of anonymity and the threat of data surveillance.

5.3 Digicash

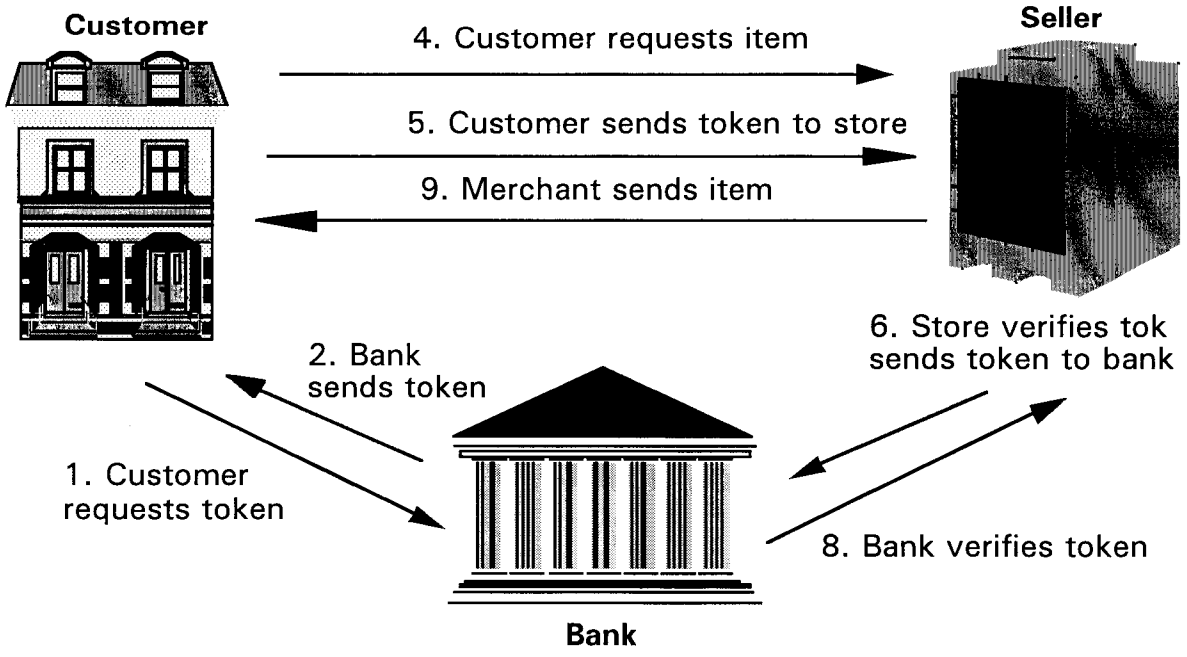
This discussion is of the original proposal for Digicash (Chaum 1985, Chaum, 1992). Additional proposals for Digicash, including a proposal based on the difficulty of finding logarithms and an off-line version, have been published. Therefore this analysis should not be considered a basis for rejecting current Digicash proposals.

In Digicash the customers themselves hold value in the form of electronic tokens. Customers and merchants exchange tokens. The tokens are validated by banks.

5.3.1 A Digicash Transaction

Digicash is a six step protocol. The specific messages as decided by the protocol are shown below. The bank has a public key consisting of b and B, where b is secret and B is published. To begin the transaction sequence the customer selects a random number r, and a number with a special form that allows it to be identified as a token. The bank uses its secret key to sign the composite number. When the customer receives this composite number back, she simply divides out the random number and has a valid, signed token.

The customer spends the token by simply sending it to the merchant. The merchant uses the bank's published key to check the format of the token. The merchant then deposits the token in the bank. The bank can recognize the token as the one previously signed, and verifies that it has no been previously spent. The token received by the bank in step five cannot be identified as the same token sent out in step two. This is the critical element which makes Digicash anonymous.



A Digicash Transaction

5.3.2 Transaction Reliability and Security

Digicash transactions are not ACID (Yee, 1994).

If the Digicash protocol is interrupted between step four and the delivery of goods to the customer, then the customer has effectively been defrauded. Since the customer is anonymous, he or she cannot simply contact the merchant and ask for the goods to be resent. (The loss of anonymity possible with web browsers has a positive effect here in that merchants could send a second time to the same virtual location.) The merchant could also claim not to have received a token, while depositing the token. In this case the customer is again defrauded. In no case does the customer have any receipt or any basis for complaint other than his or her own testimony.

There is no provision for the delivery of goods in the Digicash protocol. This creates the same opportunity for fraud and stonewalling as previously described. In the case of Digicash there is also no way for a Digicash customer to prove that the goods were ordered.

5.3.3 Implications of a Security Failure

If a Digicash banking server losses its public key then an attacker holding this key could create money at will. The ability of this system to detect a counterfeiter is questionable.

When the loss of a key was detected this would appear to invalidate every token created using that key. Digicash provides no way for the valid and fake tokens to be distinguished, or for valid customers to identify their transactions given the current design of the system.

If a customer loses her key and the authentication information to the bank then the attacker could empty the customer's account.

5.3.4 Privacy

Digicash provides an exceptionally high level of privacy. There is no way to back track the exchanges of a token in a Digicash transaction. Trapping and tracing the appropriate packets is no easier than tracing a dollar bill by its serial number.

5.4 First Virtual

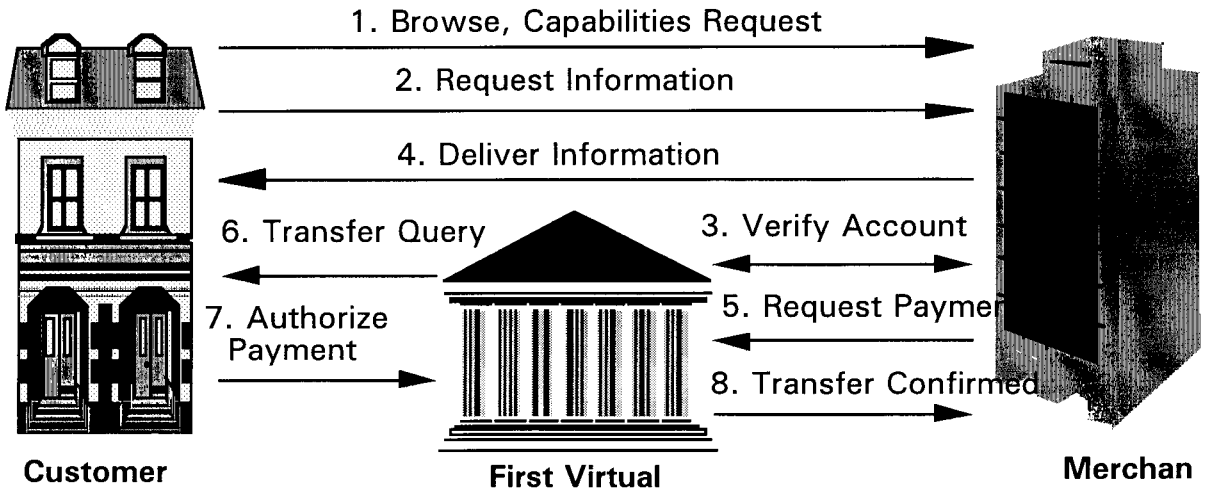
First Virtual is built on the assumption that the provision of information goods over the Internet is sufficiently inexpensive that merchant losses in an unreliable transaction protocol are negligible (First Virtual, 1995). First Virtual aggregates transactions, provides billing, and resolves disputes. The lack of reliability in First Virtual is a conscious design choice, not a design flaw. As a result of this tolerance for failure, First Virtual was the first system to be ready for widespread use.

First Virtual resolves disputes by maintaining that the customer is always right. First Virtual does charge customers a fee for declining to pay for information goods, and limits the customer's total number of refusals.

5.4.1 A First Virtual Transaction

Recall while considering this protocol that First Virtual's transaction are not built to be atomic. The lack of atomicity is not a design failure. Here again the customer is assumed to be female and the merchant male for clarity of exposition.

A First Virtual transaction begins as a customer browses and requests information from a merchant. Note that First Virtual was designed to sell information goods. The customer identifies herself with the information request with a First Virtual identifier. The customer provides a password to prove that she is a valid First Virtual customer.



First Virtual Transaction

After verifying that the customer is indeed a First Virtual customer, the merchant delivers the requested goods. The merchant then requests payment from First Virtual. First Virtual then sends email to the customer to verify the merchant's claim that he made a sale. The merchant has to wait until the customer has verified release of the funds through email to receive payment.

These steps are shown in the diagram above.

5.4.2 Transaction Reliability and Security

The customer has the right to refuse to pay for an item after having received it. This prevents conflicts based on quality and deceptive advertising. First Virtual reserves the right to limit the number of times a consumer may choose not to purchase an item received; but a merchant can not choose to refuse to offer an item to a valid First Virtual customer.

If the transaction is successful, the customer receives the merchandise. In First Virtual if a customer's account is debited then a merchant's account is credited.

Clearly the opportunity for customer fraud is large. Similarly, the opportunities for attackers to commit fraud are many. An attacker need only trap a packet which has the name of a First Virtual account holder to receive information free. Since there are well-known locations which receive many of these packets (for example, the First Virtual Infohaus) it is reasonable to assume that finding such a packet will not be difficult. Thus, First Virtual depends on the honesty (or computer illiteracy) of the majority of Internet users and criminal penalties to deter fraud.

The merchant gets the customer identity information, so merchants may easily build detailed consumer profiles. In fact, merchants are required by First Virtual to keep detailed transaction records for at least three years after the transaction (First Virtual, 1995). Since no messages are encrypted, an attacker could also develop a detailed profile of a customer's habits. Attackers could even more easily profile the accounts of a given merchant's customers and the sales of that merchant by watching only one server location.

First Virtual does provide atomic monetary transactions. However, the price is a high risk of fraud for the merchant and a complete lack of privacy for all parties.

5.4.3 Implications of a Security Failure

If a First Virtual server is subverted then fake verifications can be produced. If an attacker subverted the server, then the attacker could certainly know the email addresses of customers and could fake return replies. After the customers were charged for the fake transactions the subversion would be detected. Since charges have to go to the users at a rate set by VISA and Mastercard the fraud would be detected as soon as a flawed credit report was received by the customer.

Even with the fake verifications, the merchant would have to wait for the completion of a billing cycle to obtain funds. Because the funds are transferred to a First Virtual account and not made available as demand deposits, the fraud would be detected before the merchant was paid. Thus, First Virtual is fairly secure in that attackers have no incentive for fraud.

5.4.4 Privacy

First Virtual has complete information about every customer's transaction. First Virtual merchants are required to keep detailed records of transaction for possible dispute resolution. First Virtual must be able to obtain the item purchased in case of disputes. First Virtual merchants are under no contractual obligation to keep their information secret. In short First Virtual provides poor privacy, if any.

6 Business Opportunities

There are two great drivers of the business opportunities in electronic commerce: transactions costs and customers. These drivers have to be considered when planning entry into electronic commerce. Both lower transaction costs and better access to customers will create new markets.

With electronic commerce transactions costs can be driven down an order of magnitude. Mircomarkets that previously could not exist will become practical. Books by the page, journals by the article and individually-printed images selected from the catalogues of great world museums all are becoming economically feasible with emerging technology.

The financial services industry can offer increasingly tailored service, as well as better targeting advertising. Services which were previously brokered could be marketed directly and competitively by banks. With the World Wide Web, customers can effortlessly search for products by item name (ex. tent), purpose (ex. camping), distributor (ex. Campmor) or manufacturer (ex. Eureka). The same search capacity can extend to investment products, with customers interactively selecting an individual balance of risk, acceptable return and other elements of personal financial strategies.

Electronic commerce will allow financial institutions to provide a new class of services. For example, a bank consortium could set up a mortgage calculation page where individuals could select the financial institution best suited for their borrowing needs. Software could analyze the input of the application and select those bank and borrowing programs best suited for the applicant. Any applicant who might fail the banks' basic test could be directed to information on how to improve the application.

Provision of information services over the Web provides opportunities for banks to serve customers in a way that might be too intrusive or expensive without the network. Provision of services through networks can dramatically increase the trend to individually tailor financial services by lowering the cost of providing individual services.

7 Conclusions

The change in form from the first generation of physical currency, i.e. metal, to the next generation, i.e. printed notes, was the superficial mask on a more fundamental change in

financial systems. Changing from paper to electrons harbors equally great changes in markets and business practices that will not become apparent until electronic commerce matures.

Security, privacy and reliability are essential in electronic commerce. All of these issues must be considered in the design stage. Security and reliability cannot be provided entirely in implementation. Decisions about data compilations, including the security and disclosure of data compiled, should be made before any system trials.

Although grouped together as electronic commerce, on-line protocols for Internet commerce and off-line systems are fundamentally different. Off-line and on-line electronic commerce systems are different solutions to different problems.

Off-line systems are a solution to the problems of insecure point of sale devices. Insecure devices with physical presence have created great opportunities for fraud. ATM machines are targets; disbarred merchants share terminals; and credit, debit, and calling card fraud abounds. Off-line systems can be integrated into the current credit card infrastructure. Off-line systems can be effective in reducing merchant fraud by requiring merchant terminals to validate themselves to the cards. Off-line systems could replace point of sale purchases. The off-line market must be entered gradually through the distribution of hardware.

On-line techniques are a solution to the problems of telephone and mail order fraud. On-line techniques can replace mail order and telephone order requests with systems having higher security. On-line systems offer extremely low transaction costs and simplify the provision of personalize products. Mail order and telephone order requests are an easy target for fraud due to the lack of physical presence. Proposed on-line systems are built with the assumption that there is no physical presence. The on-line systems offer the instant provision of access to accounts to millions of users.

On-line systems offer more than the solution to the problem of current insecure remote transactions. Only on-line systems have the potential to offer an entry into the full range of financial opportunities created with electronic commerce.

The decisions to offer off-line and on-line electronic services are discrete. Every company needs to understand the potential drawbacks to both options before choosing either, or

both. While the promise of profit is great; the potential for disaster exists in equal measure. The greatest hazard may not be the unfamiliarity of electronic commerce; but the superficial similarities that can obscure subtle but significant differences.

8. References

Brands, S., 1993, "Untraceable off-line cash in wallet with observers", *Advances in Cryptology - CRYPTO '93,* Springer-Verlag: Berlin, pp. 302-318.

Business Week, 1993, "ATM shouldn't stand for 'artfully taken money'", *Business Week* (Industrial/Technology Edition), May 31, pp. 110.

Camp, L. J., 1994, "Privacy: from abstraction to applications", *Computers & Society,* September, Vol. 24, No. 3, pp. 8-15.

Camp, L. J., Marvin S. & Tygar, J. D., 1995, "Models of electronic currency", *Usenix Workshop on Electronic Commerce,* July, New York, NY, proceedings in preparation.

Chaum, D., 1985, "Security without identification: transaction systems to make big brother obsolete", *Communications of the ACM,* Vol. 28, pp. 1030-1044, October.

Chaum, D., 1992, "Achieving electronic privacy", *Scientific American,* Vol. 267, pp. 76-81.

Chaves, C., 1992, "The death of personal privacy", *Computerworld,* pp. 25 - 27, January.

Compaine B. J.,1988, *Issues in New Information Technology,* Ablex Publishing; Norwood, N. J.

Cox, B., Tygar, J. D. & Sirbu, M., 1995, "NetBill security and transaction protocol, " *Usenix Workshop on Electronic Commerce,* July, New York, NY, proceedings in preparation.

Cross Industry Working Group, 1995, "Electronic cash, tokens and payments in the national information infrastructure", *http://www.cnri.reston.va.us:3000/XIWT/documents/dig_cash_doc/ToC.html,* September

Davies, 1981, *The Security of Data in Networks,* IEEE Computer Society Press: Los Angeles, CA.

Denning, D., 1982, *Cryptography and Data Security,* Addison-Wesley Publishing: Reading, MA.

Dowling, M.,1993, "When you know too much", Catalog *Age,* Vol. 1, 73-75, October.

Duncan G. & Lambert D., 1989, "The Risk of Disclosure For Microdata", *Journal of Business and Economic Statistics,* Vol. 7, 207-217.

Echikson, W., 1994, "French risk it all on a smart card," *Boston Globe,* February. 28, pp. 17:2.

Feige, U., Fiat, A. & Shamir, A., 1987, "Zero knowledge proofs of identity", *Proceedings of the 19th ACM Symposium on Theory of Computing,* pp. 210-217.

Fenner, E, 1993, "How mortgage lenders can peek into your files", *Money,* pp. 44-48, April.

First Virtual, 1995, *Information About First Virtual,* http://www.fv.com:80/info, August.

Fischer, M. J., 1988, "Focus on industry", *Journal of Accountancy*, pp. 130-134, June.

Gray, J. & Rueter A., 1993, *Transactions Processing: Concepts and Techniques*, Morgan Kaufmann Publishers: San Francisco, CA.

Hansell S., 1995, "Mastercard Joins Banks to Plan Card That Works Like Cash", *The New York Times*, August 17, 1995, pp. D2.

Harrison, C., 1994, "Shoppers urged to guard against credit card fraud," *Atlanta Constitution*, December 27, pp. C4:5.

Hatch, D., 1993, "The assisted suicide of database marketing", *Target Marketing*, Vol. 16, pp. 8-9, October.

Hendricks, E., 1994, "Financial privacy", *Credit World*, Vol. 83n2, 26-27, Nov./Dec.

Longo, T. 1995, "Are your financial secrets for sale?", *Kiplinger's Personal Finance Magazine*, Vol. 49, pp. 117-118, April.

Low, S., Maxemchuk, N. F., & Paul, S., 1993, *Anonymous Credit Cards*, AT&T Bell Laboratories; Murray Hill, N. J.

Madsen, W., 1992, *Handbook of Personal Data Protection*, Stockton Press: New York, N.Y.

Markoff, J., 1995, "Security flaw is discovered in software used in shopping," *The New York Times*, September 19, pp. A1, D21.

Mayland, P. F., 1993, "EFT network RISK begs CEO attention", *Bank Management*, Vol. 69, pp. 42-46, October.

McLean, E., 1994, "Privacy big issue for mailers", *Advertising Age*, Vol. 65, July 4, pp. 14.

Micali, 1993, *Fair Public-Key Cryptosystems*, Laboratory for Computer Science, Massachusetts Institute of Technology: Cambridge, MA.

National Institute of Standards and Technology, 1994, *Federal Information Processing Publication 185: Escrowed Encryption Standard,* United States Government Printing Office: Gaithersburg, MA.

National Computer Security Center, 1985, *Trusted Systems Evaluation Criteria DOD-5200.28-STD,* United States Government Printing Office: Gaithersburg, MA.

NECX Direct, 1995, *Fourth Floor: Personal and Professional Service*, http://www.mecklerweb.com/imall/4-servcs.html.

Neuman, B. C. & Medvinsky, G., 1995, "Requirements for network payment: the NetCheque perspective", *IEEE ComCon,* San Francisco, CA; March 6.

Okamoto, T. & Ohta, K., 1991, "Universal electronic cash", *Advances in Cryptology-CRYPTO '91,* Springer-Verlag: Berlin, pp. 324-336.

Rivest, R. L., Shamir, A. & Adleman, L., 1978, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the ACM,* Vol. 21, pp. 158-164.

Ross, C., 1995, "Take steps to guard financial privacy", *Atlanta Constitution,* July 10, E5:3.

Sandberg, J., 1995, "Netscape software for cruising Internet is found to have another security flaw", *The Wall Street Journal,* September 25, pp. B12.

Schneier, B., 1994, *Applied Cryptography*, John Wiley & Sons, Inc., New York, NY

Schnorr, C. P., 1990, "Efficient signature generation of smart cards", *Advances in Cryptology-CRYPTO* '89, Spring-Verlag: Berlin, pp. 239-252.

Shamir, A., 1979, "How to share a secret", *Communications of the ACM,* Vol. 22, pp. 612-613.

Sirbu, M., & Tygar, J. D., 1995, "NetBill: an Internet commerce system optimized for network delivered services", *IEEE ComCon,* San Francisco, CA; March 6.

Tygar, J. D. & Yee, B., 1991, "Strongbox: a system for self securing programs", *CMU Computer Science: A 25th Anniversary Commemorative*, ed. R. Rashid, 1991, Addison-Wesley and ACM Press: New York, NY, pp. 163-198.

Van Natta, D., 1995, "5 phone marketers arrested in CREDIT card sting", *New York Times*, August 15, A, 14:2.

Yee, B. S., 1994, *Using Secure Coprocessors*, Carnegie Mellon University. School of Computer Science, CMU-CS-94-149, School of Computer Science, Carnegie Mellon University: Pittsburgh, PA.