82-10-25 An Introduction to Electronic Commerce for Financial Institutions
Carol A. Siegel

Payoff
Information security must be fully integrated into the development life cycle of any electronic commerce (EC) application. Companies need to be fully aware of the new technologies and the options for using various payment methods on the Internet. This article presents an array of today's Internet-based EC solutions from a security perspective. It focuses on consumer-to-business type transactions and presents a prediction for where Web-based financial services are going in the future.

Introduction
Today, Internet-related electronic commerce (EC) is less than 1% of total electronic commerce business. By the year 2000, this number is expected to rise to 20%. The financial services industry plays a small part in that number, but this situation is changing. Now, it would be difficult to find a major financial services company that is not seriously considering Web-based services. Moreover, what has been the major obstacle to providing these new services? Security. Corporations are worried that their internal networks may be threatened by hackers who may steal information or plant viruses. This fact makes it a particularly interesting time for information security professionals, as they are now squarely placed on the critical path of any Internet project. No longer can the business side of an operation consider the information security of its applications to be unimportant. Information security must be addressed as any other critical success factor, and must be fully integrated into the development life cycle of any EC application.

This article presents an array of today’s Internet-based EC solutions from a security perspective. It discusses the payment technologies that can be used on the Internet, such as credit cards, electronic currency, and smart cards. It also introduces the key players who are offering solutions in each of these arenas. It focuses on consumer-to-business type transactions, such as those used for home shopping and online financial services, and it presents a prediction for where Web-based financial services are going in the future. In a continuation of the electronic commerce discussion, Article 82-10-26 describes a methodology to use when integrating security considerations into electronic commerce procedures.

Electronic Commerce Payment Solution Providers
Electronic Commerce (EC) solution providers can be divided into four categories: credit card clearing capabilities, electronic money systems, debit systems, and financial services. Financial services include banking, bill paying, and brokerage services. Note that these categories are not mutually exclusive.

Credit Card Clearing Solution Providers
These companies provide organizations with a turnkey solution, help customize a package, or assist in building a solution from scratch. Some of the leaders in this area that have comprehensive EC product lines are:

- **Netscape Communications Corporation.** Netscape was the first company to provide a secure solution for EC, and, to date, its browser still has the greatest market
share. It has a commerce server line based on the Secure Socket Layer (SSL), an open standard that was developed in-house. It also has a certificate server based on RSA public key cryptography and X.509 (an ANSI open standard).

- Microsoft Corporation. Microsoft recently changed its direction to integrate Internet services into a majority of its products. It now has a comprehensive EC product line.

- Open Market. This company makes secure Web servers and back office solutions.

- IBM. IBM offers a full range of EC servers and software solutions.

- Terisa Systems. They have a secure Web toolkit that can help build branded solutions.

Other companies, such as CyberCash, Inc., offer authorized credit card and proprietary money payment services. CyberCash was founded by Bill Melton (who was also the founder of VeriFone), and Dan Lynch (founder and chairman of Networld/Interop). CyberCash went public in 1996, and has been a big success story. To use the CyberCash system, both the merchant and the customer have to have CyberCash software loaded onto their PCs. When the customer decides to make a purchase, he or she selects a credit card. The CyberCash software then encrypts the customer's credit card information and sends it to the merchant over the Internet. The encryption that CyberCash uses is 56-bit DES together with 768-bit RSA. The customer's information is then combined with merchant identification information, encrypted, and sent to a CyberCash payment server for verification. If verified, CyberCash performs a standard credit card request to the merchant's bank or bank-designated processing center. The merchant's bank processes the request through the credit card association and the cardholder's bank. After approval, the CyberCash server sends an electronic receipt with credit card authorization back to the merchant. To complete the transaction, the merchant sends a confirmation to the customer. CyberCash's systems are used by Wells Fargo's credit card merchants through the Wells Fargo Mall. Other financial institutions using CyberCash include Mellon Bank, First Union, and First USA. In addition, Spry, CompuServe, and CheckFree have integrated CyberCash's software into their Internet browsers.

From the merchant's perspective, there are online authorization systems that verify customer credit cards over the Internet. The leaders in this area are:

- IC Verify. This company offers a PC-based software solution.

- Credit Card Network. They use Netscape's commerce software together with a direct link to VISAnet.

- VeriFone. A major vendor of point-of-sale systems, now extending its services to Internet commerce solutions. It has alliances with Netscape and Oracle to create a secure Web payment server.

Another major player is a company called First Virtual Holdings (FV). They have what is called an offline credit card processing system. Both consumers and merchants have to have FV accounts that they have set up offline, either by mail or telephone. The actual credit card processing is handled offline by FV and not over the Internet. All transactions between the consumer and the merchant are initiated and confirmed by Internet E-mail. A buyer has the opportunity to confirm all purchases before his or her credit card is actually charged, and merchants are not paid for 91 days. FV's underlying philosophy is that the Internet is not safe to handle credit card processing directly; therefore, it does all its
processing offline. The FV system also supports what are called “micropayments.” Micropayments are fractions of a cent that can be used to pay for smaller items, such as a newspaper article. This capability has important implications for the publishing industry, and may be used as well in the future for accessing pages of information on Web servers.

**Electronic Currency**

With the advent of the digital age, widespread use of digital cash is inevitable. Historically, electronic money is not new. It has been used for Automated Clearing House (ACH) functions and electronic funds transfer for quite some time. However, actual digital currency is relatively new. The leader in developing electronic currency is a company called DigiCash, Inc. DigiCash, founded by Dr. David Chaum, holds the patent for “e-cash.” E-cash is digital cash—strings of zeros and ones that represent coins of varying denominations. DigiCash’s goal is to enable financial institutions to issue their own digital bearer instruments by licensing the DigiCash technology.

Digital coins are designed to be the electronic equivalent of hard currency. They act as “cash” in that they are anonymous. What makes them anonymous is the way in which cryptography is used to shield the owner of the coin. The coins are “held” inside a cryptographic envelope that prevents any of the players in the transaction (i.e., the consumer’s bank, the merchant, or the merchant’s bank) from discovering who owns the coins. This feature makes the digital coins anonymous like hard currency. Due to this technique, Dr. Chaum calls them “unconditionally untraceable.”

To use the system, both customers and merchants need either DigiCash's software or a bank's software that has a license from DigiCash. A customer requests a download of digital cash from his or her bank account to a Personal Computer (PC). The software on his or her PC creates blank coins and assigns unique serial numbers to each coin to prevent future coin reuse. The DigiCash software can also recreate these serial numbers from a seed that was recorded during account installation. This feature is another safety measure of the system that enables the coins to be re-created in the case that the customer's PC crashes.

The blank coins are sent to the customer's bank, hidden in the cryptographic envelope described earlier. Remember that, as a result of this cryptographic envelope, the bank does not know who sent the coins. Upon receipt of the coins, the bank digitally signs them for validation and assigns value to them. The bank signs them “blindly,” because they are shielded from the bank in the encryption envelope. The bank then sends the coins back to the customer, who pays the merchant with them over the Internet as well. To complete the loop, the merchant sends the coins to his bank for verification.

The DigiCash system is currently being used by Mark Twain Bancshares, EUnet (a European Internet Service Provider), and is in trial at Deutschebank. Interestingly, Mark Twain's e-cash capability is that a consumer's transactions lose their protection by the Federal Deposit Insurance Corporation once money has been converted from dollars from his or her direct-deposit account to an e-cash deposit account. The lack of FDIC protection in this case comes to the crux of the matter. These new forms of money need to be sanctioned and accepted by regulatory agencies, as well as by the government, before they can be universally used and accepted.

**Financial Services**

Many financial services companies that provide credit card, bill paying, or brokerage services now wish to offer these services over the World Wide Web. Furthermore, many companies that previously specialized in one type of service, such as bill paying, also wish to expand their service line to satisfy all their customers' financial needs. A good example of this is the CheckFree Corporation. CheckFree is best known for its bill-paying services and it has a substantial portfolio of Fortune 100 companies. Recently, it added Internet-
based home banking and corporate banking to its lines of business. The merger with Security APL has enabled CheckFree to offer PAWWS portfolio management software as a bank-branded solution. Their Web-based BankAtHome product offers account balance, account history, bill history, funds transfer, and bill paying capabilities. For security, CheckFree uses the Netscape Commerce Server in conjunction with the CyberCash security system. The BankAtHome product is being used by Bank of America and Nationsbank.

For Internet-based banking, virtual banking on the Net is the ultimate goal. Security First Network Bank (SFNB) is doing it today. SFNB was created in October, 1995 and is the first virtual bank on the Internet. It has no physical “brick and mortar” locations at all. As of the second quarter of 1996, they had signed up more than 3,000 customers in 50 states. SFNB offers Internet-based checking, credit card and loan applications, mutual funds, insurance, and bill paying (by using the CheckFree services) and provides brokerage services (i.e., portfolio, research, and market trends) through Macro*World. The two companies behind its banking systems are Five Paces, Inc. and SecureWare, Inc., which SFNB has purchased. Five Paces provides the financial service software for the Virtual Bank Manager (VBM) product and SecureWare supplies the security systems. SecureWare’s systems are based on Hewlett Packard’s (HP) trusted operating system called CMW+. This system is the first commercial implementation of a highly secure operating system previously used only by the government. SFNB also sells its VBM product as a turnkey or customized solution to other banks. Other banks that are following their model are: Huntington Bankshares, Area Bancshares, and Atlanta Internet Bank. More are sure to follow.

Debit Systems

Debit type systems include the use of cash cards, check cards, electronic checks, and electronic wallets. Cash cards are also referred to as stored value cards, smart cards, or chip cards. The cards themselves can be magnetic strip in nature or can contain a microchip, depending on the role they play. They can be separate cards or have their debit functionality added to an existing card, such as an Automatic Teller Machine card, a credit card, or even an ID card. They can be disposable or rechargeable. If rechargeable, they can be loaded with value at a specialized terminal, an ATM, or directly from the Internet, depending on the application. Cash cards will undoubtedly play an increasingly important role as a payment instrument in the future. Historically, they have been used for transit systems and telephone systems, but their use as a general payment instrument will develop as they become more accepted by the public.

One of the leaders in the cash card business is Visa International. The Visa Cash Card made a major debut at the 1996 Summer Olympics, where it could be used at most merchants in the Atlanta area. To provide the cards, Visa worked with First Union, NationsBank, and Wachovia. In a similar fashion, MasterCard is also entering into the cash card business and is running card trials in Australia. American Express and Discover are following suit as well.

Another leader in the smart card business is Mondex. Mondex is a multinational electronic money system created initially by NatWest in conjunction with British Telcom and Midland Bank. Although it is a proprietary solution, some feel that it will become the standard for electronic cash systems. To use the Mondex system, users and merchants have to have Mondex software loaded on their computers. Mondex cards can be loaded up with electronic cash from PCs equipped with card-reading devices. VeriFone, the leading manufacturer of point-of-sale card readers, has now included hardware and software in its product line that is compatible with the Mondex system. VeriFone’s smart card system products permit retail merchants and consumers to use Mondex smart cards for digital cash payments. The Mondex card can be used to pay merchants over the Internet as well as in
peer-to-peer transactions between consumers without involving a merchant or bank. The system is currently being used in Swindon, England, and in San Francisco, CA, by Wells Fargo. In Canada, the Royal Bank and Canadian Imperial Bank of Commerce (CIBC) have franchised the technology. In the later part of 1996, it will be tested in Hong Kong. Mondex is also discussing its options with MasterCard and AT&T.

Representing financial institutions, the Financial Services Technology Consortium (FSTC) is conducting their own EC development efforts. FSTC is a consortium of financial services providers, universities, and government agencies. It is a nonprofit organization that sponsors collaborative research and development on interbank technical projects affecting the financial services industry, primarily with respect to the National Information Infrastructure (NII). Member banks include: Wells Fargo, Bank of America, Citicorp, First Interstate, CoreStates, Bank of Boston, The Chase Manhattan Bank, Huntington Bancshares, and Bank One. One of the FSTC's major projects is the electronic check, which goes into pilot in the beginning of 1997. This project's goal is to provide the ability to enable all-electronic checks transactions over the Internet. The electronic check uses encryption and a technology called digital signature to verify the authenticity of the customer, the merchant, and the bank at each step of the transaction. The digital signatures of the participants are certified by BBN Planet Corporation, a subsidiary of BBN Inc., who is acting as a certification authority (CA). The electronic check concept is important for the banking industry because it uses a technology that builds on their existing check infrastructure.

A new term coined by the EC age is the “electronic wallet.” In general, an electronic wallet can come in two forms: an online wallet and a wallet on a chip card. The online version is a client application that a consumer can click on when initiating a payment over the Internet. The wallet application allows consumers to store their credit cards, debit cards, electronic checks, and cash in one place. It facilitates the payment process so that users do not have to enter in a credit card number each time that they make a purchase—they just click on a specific option in the wallet. It automatically takes care of the security issues like managing the consumer's digital credentials. The other form of wallet is a chip card. The chip card operates like the online application, but adds mobility to the wallet by enabling the consumer to use the wallet in point-of-sale terminals or other PCs. Companies like VeriFone, CheckFree, and Visa have electronic wallets. The concept of the electronic wallet is becoming more well known as consumers become more familiar with and accepting of the technologies.

Concerns Regarding Internet-Based Electronic Commerce

The main obstacle to implementing full Internet-based financial services has been concerns stemming from the inherent lack of security on the Internet. Privacy and legal considerations within the overall security context are also at issue. The nature of these concerns includes four perspectives: the consumer, the merchant, the financial institution, and the government.

The Consumer

The greatest concern of consumers is stolen credit card numbers or personal information. If a consumer loses a credit card, he or she reports it to the credit card company and cancels the account. However, what if the consumer does not know that the card has been stolen? If it is stolen off the Internet or a vendor's PC, the consumer might not know until much damage has been done. In addition is the issue of deposit insurance: whether digital money deposited into a bank is insured by the FDIC.

If a credit card number is stolen, and the consumer reports it within a certain time frame, he or she is liable for only $50. What about digital money on cash cards or on PCs?
If the card is lost or stolen or a hard disk crashes, can the consumer get his or her money back? DigiCash says that its software can replace coins if a hard disk crashes. Consumer protection and credit card liability are covered under the Federal Reserve's Regulation E. It is questionable if Regulation E, in its present form, can be applied to smart cards that hold electronic cash. A new Federal Reserve proposal in development exempts stored-value cards carrying amounts up to $100 from Regulation E paperwork requirements, such as issuing receipts for each transaction and sending monthly statements of all transactions to consumers. In the proposal is also the plan to absolve card issuers of liability if consumers lose their card. If the new proposal becomes official, it may help card issuers in that they have fewer reporting requirements, but, on the other hand, consumers may be less likely to accept the new instrument.

This situation brings up the issue of trust in these new forms of cash. Trust is necessary on two levels. First, for digital cash and electronic money to work, the public must accept these new instruments without completely understanding the way in which they work. It took a long time for the public to accept the ATM card. In a sense, they need to have blind faith that these new instruments are operating the way in which they were intended. The security technology is so complicated that one has to have studied cryptography to understand how the systems work. Not only do consumers have to trust the vendors, but also they have to trust the reviewers of the systems, such as the industry professionals.

Another issue that concerns consumers has to do with remaining anonymous. Consumers would probably like to be more anonymous than they are today. In the example of hard currency, it is anonymous, for the most part. What would happen, if, in five years, electronic cash replaces hard currency? With electronic transactions, the technical capability exists to record everything. Therefore, how can anyone be sure that he or she is not being recorded?

Because of the nature of Internet, it is inherently open with little privacy. With the Web tracking software that is currently available, one should probably assume that every move can be potentially tracked and recorded. Such moves include not only executing electronic transactions, but also cover visits to newsgroups and other sites. Considerable legislation exists regarding privacy and consumers' rights. The problem is that most of it was written for other forms of media, such as print or TV, and may not be applicable. Many laws will have to be updated with respect to the Internet.

**The Merchant**

One of the merchant's greatest concerns is fraud. Merchants need assurance that the parties in the transactions are who they say they are and that the transactions are valid. Merchants also have to be concerned with their own security practices; that is, the security on their PCs and internal networks. If they are storing credit card numbers or customer data on their servers, they are legally required to protect it.

Vendor liability is also a major concern for merchants. They have to comply with regulations on who they can sell their merchandise to and what kind of merchandise they are processing. The Decency Act of the new telecommunications law is of concern to many merchants.

Timely settlements are important as well. The merchant needs assurance that he will get paid on time and that there are mechanisms to handle transactions that are disputed and items that are returned.

**The Financial Institution**

From the financial institution's perspective, fraud is always the major concern. There is a system of internal controls against fraud on back-end financial systems. However, the
Internet is being used as a front-end processor for these back-end systems. A new control structure must be built into the system to process the transactions before they enter into the existing bank infrastructure.

Financial institutions are required by the Securities and Exchange Commission (SEC) and the Federal Reserve to maintain adequate levels of security. Due to the unsecured nature of the Internet, banks are concerned that their internal networks may be penetrated by hackers. By opening up their internal networks to the Internet through a publicly registered address, banks are setting themselves up for a wide-scale attack. Tremendous amounts of money are being spent on developing firewall technology, but firewalls alone are not the answer. Any dial-up line into the internal network may be an entry point for an intruder. Solid baseline controls are essential to any Internet security program. Some organizations are being lured into a false sense of security by thinking that a firewall will provide all the protection necessary.

There are many security issues associated with offering certain Transmission Control Protocol (TCP/IP) services such as Telnet, remote login (rlogin), and File Transfer Protocol (FTP). Most organizations start by not offering any inbound services and providing limited outbound services for employees. However, as they start to require more Internet functionality due to increasing demands for EC, companies may be forced to permit some of the less secure services. Particularly important to a bank is its image and reputation. Even a slight modification of a home page can result in a severe blow to a bank's reputation and possibly translate into dollar losses.

Another issue is that of nonbanks. Previously mentioned was the need to update Regulation E so that it applies to new technologies, such as the cash card, in addition to the FDIC issue with respect to digital money. Will Regulation E and the FDIC cover nonbanks? Do nonbanks fall under federal banking regulations? For example, will they have to obey the reserve requirement, that is, be required to keep a certain percentage of their deposits in “reserve” and not invest or loan them? What form will nonbank participation take? Will they steal market share for financial services from traditional banks?

The Government

The government, as well as financial institutions, is worried about potential financial infrastructure collapse. Parallels have been drawn between e-cash and the defunct US banknote instrument. The banknote did not work because it was not accepted by all banks. With e-cash, if one bank failed, all its notes would be worthless. This scenario could result in a cascading effect throughout the banking system.

The government is also concerned about the lack of accountability. The e-cash systems are designed to be anonymous. In addition, banking regulations must be updated to cover these new forms of electronic money payments. A question arises about nonbanks or peer-to-peer payments in which the financial institution is out of the loop. Here, no record of the transaction may exist. This situation could potentially lead to tax evasion. Sales tax can be avoided, and large transactions may not be reported to the Internal Revenue Service (IRS). Some believe that e-cash is perfect for criminals. Money laundering would become significantly easier. With multiple anonymous payments, there may be no way to ever trace the origin of the payment. They would be truly “unconditionally untraceable.” In addition, is the issue of counterfeiting. Because e-cash is a string of bits, it can be copied. The Secret Service is very concerned about this aspect.

The government may not wish electronic cash to be widely used, because it may lose the float on hard cash that is not in active circulation, which could be cash stored away for savings, cash in vending machines, or cash taken out of the country. Anyone who is holding hard currency is, in effect, lending it to the government, which pays no interest on it. A little known fact is that the Federal Reserve is required to buy and hold Treasury securities in an amount equal to all outstanding cash. Every year, the Federal Reserve turns
over the interest that it earns on these securities (currently about $20 billion). This interest is called seigniorage. If the total dollar value of cash is reduced due to privately issued electronic cash, the government stands to lose some of this income.

Some economists predict that these new instruments may make monetary policy ineffective. By allowing nonbanks to create money in the form of electronic cash, the overall money supply is affected in two ways: it is increased as new cash is created, and the velocity of money (i.e., the rate at which money changes hands) is increased, because electronic money travels around globally at electronic speeds. The money supply and the velocity of money are related through the “equation of exchange.” These economists predict that this uncontrolled acceleration of the velocity of money could lead to financial instability. Control over the money supply is very important to the government, because the government uses it to tweak the economy.

The Financial Services Industry Internet Electronic Commerce Initiatives

The financial services industry is conservative. With a new technology, such as the Internet, the industry will undoubtably be careful. This is not just a cultural issue, but is required as a result of fiduciary responsibility. Controls dictated by the SEC, the Federal Reserve, the American Bankers Association, and others prohibit banking institutions from using systems that have specific levels of security standards and processes. As controls for Internet-based systems improve, increasingly more financial institutions will offer Internet-based services. At this time, many major US financial institutions are using many of the previously mentioned companies to provide secure solutions for EC. Even the Federal Reserve is contemplating getting involved. It is considering offering T-bills, bonds, and note services on the World Wide Web and it is also looking at providing electronic currency services.

Conclusion

As of mid 1996, many financial institutions were advertising on the Web, with some taking customer requests for loans. For the most part, financial institutions are providing information over the Internet and are taking that information to be processed offline. Some banks, such as SFNB, are doing much more. In terms of brokerage services, many companies are offering quotes, and some have started to offer online trading with limited degrees of personal information being transmitted across the Internet. In development are real-time stock exchange development efforts. The trend is to offer more and more Internet-based services, both banking and brokerage.

On the electronic cash curve, the disposable cash card and the reloadable one have already emerged. With the Mondex system, the reloading of cash cards through the Internet is possible. In the future, proprietary money systems, like Mondex or DigiCash, might expand their horizons and become the global standard, or other players may emerge. As digital monetary systems mature, they will inevitably be linked to the Internet. Although it is hard to quantify exactly when, it is possible that the year 2000 will see the emergence of a global electronic monetary system offered over the Internet in conjunction with full financial services.

Article 82-10-26 continues the discussion of electronic commerce by presenting a methodology to use when developing a security system for electronic commerce procedures.

Author Biographies

Carol A. Siegel
Carol A. Siegel is a vice president in the Internet Security & Architecture group at J.P. Morgan, Inc. She has over 12 years experience in information technology and has specialized in IT risk management, security, and audit.