

CHAPTER 11

PAYMENT SYSTEMS FOR ELECTRONIC COMMERCE

LEARNING OBJECTIVES

In this chapter, you will learn about:

- The basic functions of online payment systems
- The use of payment cards in electronic commerce
- The history and future of electronic cash
- How electronic wallets work
- The use of stored-value cards in electronic commerce
- Internet technologies and the banking industry

INTRODUCTION

In 1991, a teenager named Max Levchin immigrated from the Ukraine to the United States. Settling in Chicago, Levchin had a burning interest in cryptography. Growing up in a Soviet police state convinced him that the ability to send coded messages that could not be read or intercepted was both important and useful. He majored in computer science at the University of Illinois and spent many hours at the school's **Center for Supercomputing**, pursuing his passion for making and breaking codes. When he graduated in 1998, he wanted to follow the American dream of turning his knowledge into money, so he headed for the heart of the computer industry in Palo Alto, California. Levchin's plan to build the ultimate transmission encryption scheme has not yet panned out, but he has managed to turn his knowledge into a successful business. As cofounder and chief technical officer of **PayPal**, an online payment processing company that

you will learn about in this chapter, Levchin has used his expertise in cryptography and computer security to protect the firm from losses that could destroy it.

PayPal, founded in 1999, operates a service that lets people exchange money over the Internet. It has become the most used payment system for clearing auction transactions on eBay. People can also use PayPal to send money to anyone who has an e-mail address and to receive money.

PayPal charges very small fees to business users and no fees at all to individuals, so its profit margins are small. However, it has grown so rapidly that its thin profit margins are realized on a very large number of users. A single, well-organized, large-scale fraud attack on PayPal, however, could put the company out of business quickly. Levchin's current contribution to the company's success is his development of payment surveillance software that continually monitors PayPal transactions. The software searches millions of transactions as they occur every day and looks for patterns that might indicate fraud. The software notifies PayPal managers immediately when it finds something suspicious.

The software appears to be working very well. Companies that process credit card transactions have experienced much larger fraud occurrence rates on the Web (about 1.13 percent) than in physical stores (about .70 percent). PayPal claims to have kept its fraud rate below .50 percent. As long as PayPal can keep its fraud rate low, it can continue to charge lower transaction fees than its competitors and still make a profit. Some industry observers believe that PayPal's ability to avoid high fraud rates could make it a serious competitor to banks in other areas of financial transaction handling, such as credit card processing.

PayPal's largest customer group has always been the participants (buyers and sellers) on the auction Web site eBay. As you will learn in this chapter, eBay spent three years working to establish its own payments service that could compete effectively with PayPal. In October 2002, eBay finally gave up and bought PayPal for \$1.4 billion. PayPal continues to offer payment services under its own name as a division of eBay.

ONLINE PAYMENT BASICS

An important function of electronic commerce sites is the handling of payments over the Internet. Most electronic commerce involves the exchange of some form of money for goods or services. As you learned in Chapter 5, many companies use electronic funds transfers (EFTs) or financial EDI to make online payments. In this chapter, you will learn about a number of online payment alternatives that are available to individual consumers.

Online payment systems for consumer electronic commerce are still evolving. A number of proposals and implementations of payment systems currently compete for dominance. Regardless of format, electronic payments are far cheaper than mailing paper checks. Electronic payments can be convenient for customers and can save companies money. Estimates of the cost of billing one person by mail range between \$1 and \$1.50. Sending bills and receiving payments over the Internet can drop the transaction cost to an average of 50 cents per bill. The total savings is huge when the unit cost is multiplied by the number of customers who could use electronic payment. For example, a telephone company in a major metropolitan area might have 5 million customers, each of whom receives a bill every month. In one year, a savings of 50 cents on each of those 60 million bills adds up to about \$30 million. The environmental impact is also significant. Those 60 million paper bills weigh about 1.7 million pounds. It takes 2200 trees to make that much paper—along with the energy consumed and the wastes generated in the paper-making process.

Today, four basic ways to pay for purchases dominate both traditional and electronic business-to-consumer commerce. Cash, checks, credit cards, and debit cards account for more than 90 percent of all consumer payments in the United States. A small but growing percentage of consumer payments are made by electronic transfer. The most popular consumer electronic transfers are automated payments of auto loans, insurance payments, and mortgage payments made from consumers' checking accounts. Figure 11-1 shows the estimated proportions of the \$6.7 trillion in payments projected for 2005 in the United States for all types of consumer commerce, online and offline.

Credit cards are by far the most popular method that consumers use to pay for online purchases. Recent surveys have found that more than 85 percent of worldwide consumer Internet purchases are paid for with credit cards. In the United States, the proportion is about 96 percent.

Another payment medium is limited-use scrip. **Scrip** is digital cash minted by a company instead of by a government. Most scrip cannot be exchanged for cash; it must be

Type	Number of transactions	Dollar value of transactions
Cash	35%	15%
Checks	21%	32%
Credit cards	19%	26%
Debit cards	17%	12%
Electronic transfers	5%	11%
Other	3%	4%

Adapted from Table 1182, *2004-2005 Statistical Abstract of the United States*, Washington, D.C.: U.S. Census Bureau, p. 746.

FIGURE 11-1 Payment methods for all types of U.S. consumer transactions, 2005 projections

exchanged for goods or services by the company that issued the scrip. Scrip is like a gift certificate that is good at more than one store. In the early days of the Web, many experts predicted that scrip would become a popular way of making payments for consumer goods and services online. Unfortunately for many investors and at least two companies (see the Learning from Failures feature), this turned out not to be true. Most current scrip offerings, such as **eScrip**, focus on the not-for-profit fundraising market. This market consists mainly of primary and secondary schools in the United States.

LEARNING FROM FAILURES

Flooz and Beenz

Flooz and Beenz were two pioneers in the business of issuing scrip for use on the Web. The scrip created by these two companies could be bought, traded, and exchanged for merchandise, or discounts on merchandise, at hundreds of Web retailers.

In 1998, Beenz began offering its scrip for sale on its Web site. The scrip was called beenz, and the company's logo included a small kidney bean shape. A number of merchants agreed to accept the beenz scrip and by mid-2000, Beenz had more than a million customers who were accumulating and using beenz to buy merchandise on the Web. Beenz formed a partnership with Columbus Bank and Trust that allowed beenz holders to transfer their beenz value to a debit card that they could use in the physical world.

Flooz began selling its scrip product, flooz, in late 1999. Flooz had overwhelming support from major partners, such as NextCard, and quickly signed an agreement with BarnesandNoble.com in which the bookseller would accept flooz scrip for purchases on its Web site. Flooz undertook major promotional activities, including an \$8 million advertising campaign featuring Whoopi Goldberg.

By August 2001, both companies had ceased operations. The idea of using scrip was novel and it did give parents a way to allow their children to make purchases on the Web. However, scrip did not solve any major problems for most online buyers and it required that they learn a new and different technique for making Web payments. Another major barrier to adoption was that neither product meshed very well with existing payment systems.

continued

The lesson from the Flooz and Beenz failures is that any Web product or service must meet a real need of consumers, and it must not require those consumers to learn a new way to do something that they are already comfortable doing. The new product or service must also integrate well with existing systems and practices.

Merchants should offer their customers payment options that are safe, convenient, and widely accepted. The key is to determine which choices work the best for the company and its customers. The information in this chapter will help you make those decisions. Companies such as **Payment Online**, shown in Figure 11-2, sell packages of payment processing services to Web merchants that allow those merchants to accept several different types of payments.



FIGURE 11-2 Payment processing service offerings of Payment Online

You will learn about four different payment technologies in this chapter: payment cards, electronic cash, software wallets, and smart cards (also called stored-value cards). Each technology has unique properties, costs, advantages, and disadvantages. Some are methods that are already popular and widely accepted; others are only beginning to catch on and have an unclear future. All of these electronic payment methods can work well for B2C Web commerce sites.

PAYMENT CARDS

Businesspeople often use the term **payment card** as a general term to describe all types of plastic cards that consumers (and some businesses) use to make purchases. The main categories of payment cards are credit cards, debit cards, and charge cards.

A **credit card**, such as a **Visa** or a **MasterCard**, has a spending limit based on the user's credit history; a user can pay off the entire credit card balance or pay a minimum amount each billing period. Credit card issuers charge interest on any unpaid balance. Many consumers already have credit cards, or are at least familiar with how they work. Credit cards are widely accepted by merchants around the world and provide assurances for both the consumer and the merchant. A consumer is protected by an automatic 30-day period in which he or she can dispute an online credit card purchase. Merchants that already accept credit cards in an offline store can accept them immediately for online payment because they already have established a mechanism for accepting credit card payments. Online credit card purchases are similar to telephone purchases in that the card holder is not present and cannot provide proof of identity as easily as he or she can when standing at the cash register. Online and telephone purchases are often called **card not present transactions** and both require an extra degree of security.

A debit card looks like a credit card, but it works quite differently. Instead of charging purchases against a credit line, a **debit card** removes the amount of the sale from the cardholder's bank account and transfers it to the seller's bank account. Debit cards are issued by the cardholder's bank and usually carry the name of a major credit card issuer, such as Visa or MasterCard, by agreement between the issuing bank and the credit card issuer. By branding their debit cards (with the Visa or MasterCard name), banks ensure that their debit cards will be accepted by merchants who recognize the credit card brand names.

A **charge card**, offered by companies such as **American Express**, carries no spending limit, and the entire amount charged to the card is due at the end of the billing period. Charge cards do not involve lines of credit and do not accumulate interest charges. (Note: In addition to its charge card products, American Express also offers credit cards, which do have credit limits and which do accumulate interest on unpaid balances.) In the United States, many retailers, such as department stores and oil companies that own gas stations, issue their own charge cards. In the rest of this chapter, the term "payment card" refers to credit cards, debit cards, and charge cards.

Many consumers have concerns about providing their payment card numbers to vendors online, especially when the vendor is unknown to them. To address this concern, several payment card companies now offer cards with disposable numbers. These cards, sometimes called **single-use cards**, give consumers a unique card number that is valid for one transaction only. This prevents an unscrupulous vendor from using the card number to complete unauthorized transactions on the consumer's account or selling the card number to others. In 2000, American Express was the first to offer single-use cards. A few other card issuers followed suit, but the number of companies that offer single-use cards continues to be small. Neither Visa nor MasterCard have required all of their issuing banks to provide single-use cards; the only major issuing banks to do so are MBNA and Citigroup. J.P. Morgan offers a single-use version of its Discover card. In 2004, American Express stopped offering its single-use card, but many industry analysts believe that consumer interest in these types of cards will continue to grow. The problem with single-use cards thus far has been that they require consumers to behave differently and not enough consumers see the benefit of learning how to use this new product. As concerns over stolen credit card numbers increase, this benefit could become compelling.

Advantages and Disadvantages of Payment Cards

Payment cards have several features that make them an attractive and popular choice with both consumers and merchants in online and offline transactions. For merchants, payment cards provide fraud protection. When a merchant accepts payment cards for online payment or for orders placed over the telephone, the merchant can authenticate and authorize purchases using a payment card processing network. For U.S. consumers, payment cards are advantageous because the Consumer Credit Protection Act limits the cardholder's liability to \$50 if the card is used fraudulently. Once the cardholder notifies the card's issuer of the card theft, the cardholder's liability ends. Frequently, the payment card's issuer waives the \$50 consumer liability when a stolen card is used to purchase goods. Some other countries have similar laws, but this type of protection is not common for holders of credit cards issued outside the United States. The lack of this type of protection does limit the willingness of non-U.S. consumers to use payment cards for online purchases.

Perhaps the greatest advantage of using payment cards is their worldwide acceptance. Payment cards can be used anywhere in the world, and the currency conversion, if needed, is handled by the card issuer. For online transactions, payment cards are particularly advantageous. When a consumer reaches the electronic checkout, he or she enters the payment card number and his or her shipping and billing information in the appropriate fields to complete the transaction. The consumer does not need any special hardware or software to complete the transaction.

Payment cards have one significant disadvantage for merchants when compared to cash. Payment card service companies charge merchants per-transaction fees and monthly processing fees. These fees can add up, but merchants view them as a cost of doing business. Any merchant that does not accept payment cards for purchases risks losing a significant portion of sales to other merchants that do accept payment cards. The consumer pays no direct transaction-based fees for using payment cards, but the prices of goods and services are slightly higher than they would be in an environment free of payment cards. Most consumers also pay an annual fee for credit cards and charge cards. This annual fee is much less common on debit cards.

Payment cards provide built-in security for merchants because merchants have a higher assurance that they will be paid through the companies that issue payment cards than through the sometimes slow direct invoicing process. To process payment card transactions, a merchant must first set up a merchant account. The series of steps in a payment card transaction is usually transparent to the consumer. Several groups and individuals are involved: the merchant, the merchant's bank, the customer, the customer's bank, and the company that issued the customer's payment card. All of these entities must work together for customer charges to be credited to merchant accounts (and vice versa when a customer receives a payment card credit for returned goods).

Payment Acceptance and Processing

Most people are familiar with the use of payment cards: In a physical store, the customer or a sales clerk runs the card through the online payment card terminal and the card account is charged immediately. The process is slightly different on the Internet, although

the purchase and charge processes follow the same rules. Payment card processing has been made easier over the past two decades because Visa and MasterCard, along with MasterCard's international affiliate, **MasterCard International** (formerly known as Europay), have implemented a single standard for the handling of payment card transactions called the **EMV standard** (EMV is derived from the names of the companies: Europay, MasterCard, and Visa).

In a brick-and-mortar store, customers walk out of the store with purchases in their possession, so charging and shipment occur nearly simultaneously. Online stores and mail order stores in the United States must ship merchandise within 30 days of charging a payment card. Because the penalties for violating this law can be significant, most online and mail order merchants do not charge payment card accounts until they ship merchandise. Payment card transactions follow these general steps once the merchant receives a consumer's payment card information, which is usually sent using the SSL encryption technique you learned about in Chapter 10:

1. The merchant authenticates the payment card to ensure it is valid and not stolen.
2. The merchant checks with the payment card issuer to ensure that credit or funds are available and puts a hold on the credit line or the funds needed to cover the charge.
3. Settlement occurs, usually a few days after the purchase, which means that funds travel between banks and are placed into the merchant's account.

Open and Closed Loop Systems

In some payment card systems, the card issuer pays the merchants that accept the card directly and does not use an intermediary, such as a bank or clearinghouse system. These types of arrangements are called **closed loop systems** because no other institution is involved in the transaction. American Express and Discover Card are examples of closed loop systems.

Open loop systems involve three or more parties. Suppose an Internet shopper uses his or her Visa card issued by the First Bank of Woodland to purchase an item from Web Wonders, whose bank account is at the Hackensack Commerce Bank. The banking system includes one or more intermediary banks that coordinate the transfer of funds from the First Bank of Woodland to the Hackensack Commerce Bank. Whenever a third party, such as the intermediary banks in this example, processes a transaction, the system is called an **open loop system**. Systems using Visa or MasterCard are the most visible examples of open loop systems. Many banks issue both cards. Unlike American Express or Discover, neither Visa nor MasterCard issues cards directly to consumers. Visa and MasterCard are **credit card associations** that are operated by the banks who are members in the associations. These member banks, which are also called **customer issuing banks**, issue credit cards to individual consumers and are responsible for establishing customer credit limits.

Merchant Accounts

A **merchant bank** or **acquiring bank** is a bank that does business with sellers (both Internet and non-Internet) that want to accept payment cards. In other words, to process payment cards for Internet transactions, an online merchant must set up a **merchant account**. When the merchant's bank collects credit card receipts on behalf of the merchant from the payment card issuer, it credits their value to the merchant's account.

A merchant must provide business information before the bank will provide an account through which the merchant can process payment card transactions. Typically, a new merchant must supply a business plan, details about existing bank accounts, and a business and personal credit history. The merchant bank wants to be sure that the merchant has a good prospect of staying in business and wants to minimize its risk. An online merchant that appears disorganized is less attractive to a merchant bank than a well-organized online merchant.

The type of business also influences the bank's likelihood of granting the account. In some industries, merchant banks will be reluctant to offer a merchant account because of the type of business; some businesses have a higher likelihood of customers repudiating payment card charges than others. For example, a business that sells a guaranteed weight loss scheme—a business in which many customers might want their money back—will find many merchant banks unwilling to provide an account. The bank assesses the level of risk in the business based on the type of business and the credit information that is provided. Merchant banks must estimate what percentage of sales are likely to be contested by cardholders. When a cardholder successfully contests a charge, the merchant bank must retrieve the money it placed in the merchant account in a process called a **chargeback**. To ensure that sufficient funds are available to cover chargebacks, a merchant bank might require a company to maintain funds on deposit in the merchant account. For example, a new or risky business that plans to make \$100,000 in sales each month might be required to keep \$50,000 or more on deposit in its merchant account.

One problem facing online businesses is that the level of fraud in online transactions is much higher than either in-person or telephone transactions of the same nature (that is, the same amount and the same type of good or service being purchased). Fewer than 5 percent of all credit card transactions are completed online, but those transactions are responsible for about 50 percent of the total dollar amount of credit card fraud. A Celent Communications study reported in *Credit Card Management* (see the reference in the For Further Study and Research section at the end of this chapter) has projected that online credit card fraud will be over \$2 billion by 2007 and will amount to 62 percent of all credit card fraud.

Several third-party Internet and Web-based services are available to handle all the details of processing payment card transactions. The next section discusses payment card processing options for Internet stores.

Processing Payment Cards Online

Software packaged with electronic commerce software can handle payment card processing automatically, or merchants can contract with a third party to handle payment card processing. Several companies, called **payment processing service providers**, offer these services. **InternetSecure**, for example, allows merchants to concentrate on business

while it provides secure payment card services. InternetSecure supports payments with Visa and MasterCard for Canadian and United States accounts. The company provides risk management and fraud detection and handles transactions from online merchants using existing, bank-approved payment card processing infrastructure, secure links, and firewalls. InternetSecure notifies the merchant of all approved orders and also supplies authorization codes to buyers of digital content, who can download their purchases upon payment card approval. InternetSecure ensures that the transactions it processes are credited to the correct merchant's account.

First Data provides merchant payment card processing services with the **ICVERIFY** and **WebAuthorize** programs. ICVERIFY is intended for small retailers that use Microsoft Windows electronic cash registers and point-of-sale terminal systems. WebAuthorize is for large enterprise-class merchant sites.

Services such as ICVERIFY and WebAuthorize connect directly to a network of banks called the **Automated Clearing House (ACH)** and to credit card authorization companies. You can learn more about ACHs by following the Online Companion links to the **Electronic Payments Network, NACHA - The Electronic Payments Association, The Clearing House**, and the U.S. Federal Reserve Bank's **FedACH** site. Banks connect to an ACH through highly secure, private leased telephone lines. The merchant sends the card information to a payment card authorization company, which reviews the customer account and, if it approves the transaction, sends the credit authorization to the issuing bank. Then the issuing bank deposits the money in the merchant's bank account through the ACH. The merchant's Web site receives confirmation of the acceptance of the consumer transaction. After receiving notification of acceptance or rejection of the transaction, the merchant Web site confirms the sale to the customer over the Internet. In addition, the merchant site usually sends an e-mail confirmation of the sale to the consumer with details about the purchase price and shipping information. Figure 11-3 is a graphic representation of the process.

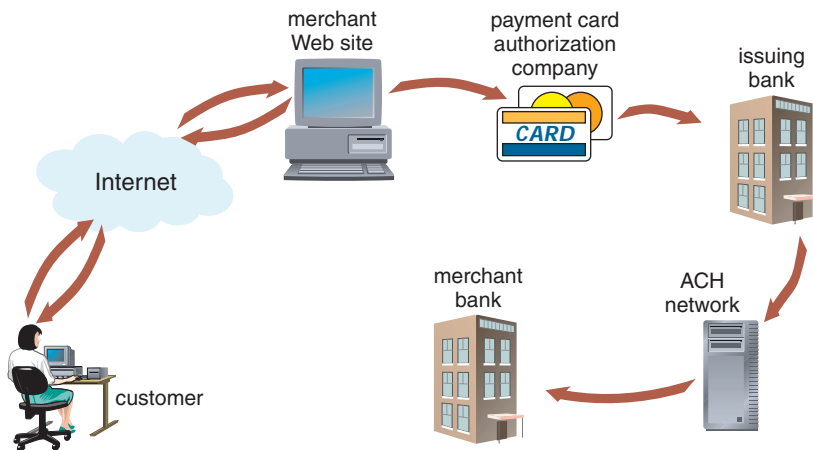


FIGURE 11-3 Processing a payment card transaction

Other payment card processing companies include VeriSign's **PayFlow Link** system and InfoSpace's **Authorize.Net**. PayFlow is an online payment system developed by CyberCash that is now operated by VeriSign. Authorize.Net is an online, real-time payment card processing service that allows merchants to link their sites to the Authorize.Net system by simply inserting a small block of HTML code into their transaction page. With Authorize.Net, a customer's order is encrypted and transferred to the Authorize.Net server. The server, in turn, relays the transaction to a bank network through a private leased line. Merchants must have an Authorize.Net account to use the service. Customers are usually not aware that the transaction is being handled by a third-party supplier. Check the Online Companion links for more details about these services.

ELECTRONIC CASH

Although credit cards dominate online payments today, electronic cash shows promise for the future. **Electronic cash** (also called e-cash or digital cash) is a general term that describes any value storage and exchange system created by a private (nongovernmental) entity that does not use paper documents or coins and that can serve as a substitute for government-issued physical currency. A significant difference between electronic cash and scrip is that electronic cash can be readily exchanged for physical cash on demand. Because electronic cash is issued by private entities, there is a need for common standards among all electronic cash issuers so that one issuer's electronic cash can be accepted by another issuer. This need has not yet been met. Each issuer has its own standards and electronic cash is not universally accepted, as is government-issued physical currency.

As you learned in the previous section, banks that issue credit cards make money by charging merchants a processing fee on each transaction. This fee ranges from 1 percent to 4 percent of the value of the transaction. Often, banks impose a minimum fee of 20 cents or more per transaction. Many banks charge electronic commerce sites more than similar brick-and-mortar stores—up to \$1 more per credit card transaction. The cost of an online transaction can be 50 percent higher than the cost to process the same transaction for a brick-and-mortar retailer.

Many stores that accept credit cards require a minimum purchase amount of \$10 or \$15. Merchants impose a minimum purchase amount because the bank fees for small purchase amounts would be greater than the profits on those transactions. The same is true for Internet purchases. Small purchases are not profitable for merchants that accept only credit cards for payment. There is a market for small purchases on the Internet—purchases below \$10. This is one potentially significant market for electronic cash. With very low fixed costs, electronic cash provides the promise of allowing users to spend, for example, 50 cents for an online newspaper, or 80 cents to send an electronic greeting card.

Electronic cash has another factor in its favor: Most of the world's population do not have credit cards. Many adults cannot obtain credit cards due to minimum income requirements or past debt problems. Children and teens—eager purchasers representing a significant percentage of online buyers—are ineligible, simply because they are too young. People living in most countries other than the United States hold few credit cards because they have traditionally made their purchases in cash. For all of these people, electronic cash provides the solution to paying for online purchases.

Even though there have been many failures in the last few years in electronic cash introductions, the idea of electronic cash just refuses to die. Electronic cash shows particular promise in two applications: the sale of goods and services priced less than \$10—the lower threshold for credit card payments—and the sale of all goods and services to those without credit cards.

Micropayments and Small Payments

Internet payments for items costing from a few cents to approximately a dollar are called **micropayments**. Micropayment champions see many applications for such small transactions, such as paying 5 cents for an article reprint or 25 cents for a complicated literature search. However, micropayments have not been implemented very well on the Web yet. Another barrier to micropayments is a matter of human psychology. Researchers have found in a number of studies that many people prefer to buy small value items in fixed-price chunks rather than in individual small increments, even when buying the small increments would cost less money overall. A good example of this behavior is the preference most mobile telephone users have for fixed monthly payment plans over charges based on minutes used. The comfort of knowing the exact amount of the monthly bill is more important to many people than getting the lowest price on the minutes used.

The payments that are between \$1 and \$10 do not have a generally accepted name (some industry observers use the term micropayment to describe any payment of less than \$10); in this book, the term **small payments** will be used to include all payments of less than \$10.

Two companies now offer products for handling small payments that use credit cards as an alternative to electronic cash. The logic behind these products is that credit cards are more widely accepted than electronic cash. **Yaga** has targeted its product to large media companies such as Hearst, Time, and Ziff-Davis. These companies want to sell copies of articles from their publications, but the transaction fees charged by credit card processors make such sales unprofitable. Yaga accumulates charges made by an individual and then processes them in one lump sum at the end of a month or longer period. If a site visitor obtained six articles in a month, Yaga allows the site to process a credit card charge once (incurring just one transaction fee) instead of six times. **BitPass** targets smaller content providers—individual authors and musicians—by offering site visitors an account that they can draw against at any BitPass participating site. A customer authorizes BitPass to make a small (usually \$3) charge to the customer's credit card to create that customer's BitPass account. The customer can then draw down the BitPass account at participating content vendor sites.

Privacy and Security of Electronic Cash

All electronic payment schemes have issues that must be resolved satisfactorily to allay consumers' fears and give them confidence in the technology. Concerns about electronic payment methods include privacy and security, independence, portability, and convenience. Privacy and security questions are probably the most important issues that have to be addressed with any payment system to be used by consumers. Consumers want to know whether transactions are vulnerable and whether the electronic currency can be copied, reused, or forged.

Electronic cash has unique security problems. Electronic cash should have two important characteristics in common with physical currency. First, it must be possible to spend electronic cash only once, just as with traditional currency. Second, electronic cash ought to be anonymous, just as hard currency is. That is, security procedures should be in place to guarantee that the entire electronic cash transaction occurs only between two parties, and that the recipient knows that the electronic currency being received is not counterfeit or being used in two different transactions. Ideally, consumers should be able to use electronic cash without revealing their identities—this prevents sellers from collecting information about individual or group spending habits. Companies in the electronic cash business include **eCharge** and **Valista**.

Electronic cash has the advantages of being independent and portable. When electronic cash is independent, it is unrelated to any network or storage device. That is, electronic cash is really not free-floating currency if its existence depends on a particular proprietary storage mechanism that is specially designed to hold one type of electronic cash. Electronic cash should ideally be able to pass transparently across international borders and be converted automatically to the recipient country's currency. Electronic cash portability means that it must be freely transferable between any two parties. Credit and debit cards do not possess this property of portability or transferability between every combination of two parties. In a credit card transaction, the payment recipient must already have a merchant account established with a bank. A merchant account is not required for a business to receive electronic cash.

Perhaps the most important characteristic of cash is convenience. If electronic cash requires special hardware or software, it is not convenient for people to use. Chances are good that people will not adopt an electronic cash system that is difficult to use.

Holding Electronic Cash: Online and Offline Cash

Two widely accepted approaches to holding cash exist today: online storage and offline storage. Online cash storage means that the consumer does not personally possess electronic cash. Instead, a trusted third party—an online bank—is involved in all transfers of electronic cash and holds the consumers' cash accounts. Online systems work by requiring merchants to contact the consumer's bank to receive payment for a consumer purchase, which helps prevent fraud by confirming that the consumer's cash is valid. This resembles the process of checking with a consumer's bank to ensure that a credit card is still valid and that the consumer's name matches the name on the credit card.

Offline cash storage is the virtual equivalent of money kept in a wallet. The customer holds it, and no third party is involved in the transaction. Protection against fraud is still a concern, so either hardware or software safeguards must be used to prevent fraudulent or double-spending. **Double-spending** is spending a particular piece of electronic cash twice by submitting the same electronic currency to two different vendors. By the time the same electronic currency clears the bank for a second time, it is too late to prevent the fraudulent act. The encryption techniques used to prevent double-spending are described later in this chapter.

Advantages and Disadvantages of Electronic Cash

Billing for goods and services that customers purchase is part of any business. Traditional billing methods in the brick-and-mortar paradigm are costly and involve generating invoices, stuffing envelopes, buying and affixing postage to the envelopes, and sending the invoices to the customers. Meanwhile, the Accounts Payable Department must keep track of incoming payments, post accounts in the database, and ensure that customer data is current.

Online stores have many of the same payment collection inefficiencies as their brick-and-mortar cousins. Most online customers use credit cards to pay for their purchases. Online auction customers also use conventional payment methods, including checks and money orders. Electronic cash systems, though less popular than other payment methods, provide advantages and disadvantages that are unique to electronic cash.

For the most part, electronic cash transactions are more efficient (and therefore less costly) than other methods, and that efficiency should foster more business, which eventually means lower prices for consumers. Transferring electronic cash on the Internet costs less than processing credit card transactions. Conventional money exchange systems require banks, bank branches, clerks, automated teller machines, and an electronic transaction system to manage, transfer, and dispense cash. Operating this conventional money exchange system is expensive.

Electronic cash transfers occur on an existing infrastructure—the Internet—and through existing computer systems. Thus, the additional costs that users of electronic cash must incur are nearly zero. Because the Internet spans the globe, the distance that an electronic transaction must travel does not affect cost. When considering moving physical cash and checks, distance and cost are proportional—the greater the distance that the currency has to go, the more it costs to move it. However, moving electronic currency from Los Angeles to San Francisco costs the same as moving it from Los Angeles to Hong Kong. Merchants can pay other merchants in a business-to-business relationship, and consumers can pay each other. Electronic cash does not require that one party obtain an authorization, as is required with credit card transactions.

Electronic cash does have disadvantages, and they are significant. Using electronic cash provides no audit trail. That is, electronic cash is just like real cash in that it cannot be easily traced. Because true electronic cash is not traceable, another problem arises: money laundering. **Money laundering** is a technique used by criminals to convert money that they have obtained illegally into cash that they can spend without having it identified as the proceeds of an illegal activity. Money laundering can be accomplished by purchasing goods or services with ill-gotten electronic cash. The goods are then sold for physical cash on the open market.

Just as physical currency can be counterfeited, electronic cash is susceptible to forgery. However, it is much more difficult to forge electronic cash than it is to use a fraudulently obtained credit card number. There are several other potentially damaging digital economic factors that might result from the use of electronic cash. These factors have to do with the expansion of the money supply when banks loan electronic cash on consumer and merchant accounts in traditional bank accounts. You can learn more about these economic factors by following the links to [Understanding the Digital Economy](#) and [The Economic and Social Impacts of Electronic Commerce](#) in the Online Companion.

Electronic cash has been successful in some parts of the world, but it has not yet become a global commercial success. Making electronic cash a popular alternative payment system requires wide acceptance and a solution to the problems of multiple electronic cash standards. Customers do not want to have to carry a dozen different brands of electronic cash to be able to purchase goods from a majority of the merchants that accept electronic cash. Establishing electronic cash as a popular payment method requires that a standard be developed for electronic cash disbursement and acceptance—a standard that individual vendors then implement for their individual electronic cash systems. Electronic cash from different vendors must be easily interchangeable so that customers can exchange one cash type for another when needed.

How Electronic Cash Works

To begin using electronic cash, a consumer opens an account with an electronic cash issuer (such as a bank that issues electronic cash or a private vendor of electronic cash, such as PayPal) and presents proof of identity. The consumer can then withdraw electronic cash by accessing the issuer's Web site and presenting proof of identity, such as a digital certificate issued by a certification authority, or a combination of a credit card number and a verifiable bank account number. After the issuer verifies the consumer's identity, it gives the consumer a specific amount of electronic cash and deducts the same amount from the consumer's account. In addition, the issuer might charge a small processing fee. The consumer can store the electronic cash in an electronic wallet (described later in this chapter) on his or her computer, or on a stored-value card (also described later in this chapter). In addition, the consumer can authorize the issuer to make payments to third parties from the electronic cash account.

Providing Security for Electronic Cash

You have already learned about one significant problem with electronic cash: its potential for double-spending. The main deterrent to double-spending is the threat of detection and prosecution. Cryptographic algorithms are the keys to creating tamperproof electronic cash that can be traced back to its origins. A two-part lock provides anonymous security that also signals when someone is attempting to double-spend cash. When a second transaction occurs for the same electronic cash, a complicated process comes into play that reveals the attempted second use and the identity of the original electronic cash holder. Otherwise, electronic cash that is used correctly maintains a user's anonymity. This double-lock procedure protects the anonymity of electronic cash users and simultaneously provides built-in safeguards to prevent double-spending. Figure 11-4 shows a graphic representation of this double-spending detection process using a double-lock system.

Double-spending can neither be detected nor prevented with truly anonymous electronic cash. **Anonymous electronic cash** is electronic cash that, like bills and coins, cannot be traced back to the person who spent it. One way to be able to trace electronic cash is to attach a serial number to each electronic cash transaction. That way, cash can be positively associated with a particular consumer. That does not solve the double-spending problem, however. Although a single issuing bank could detect whether two deposits of the same electronic cash are about to occur, it is impossible to ascertain who is at fault in such

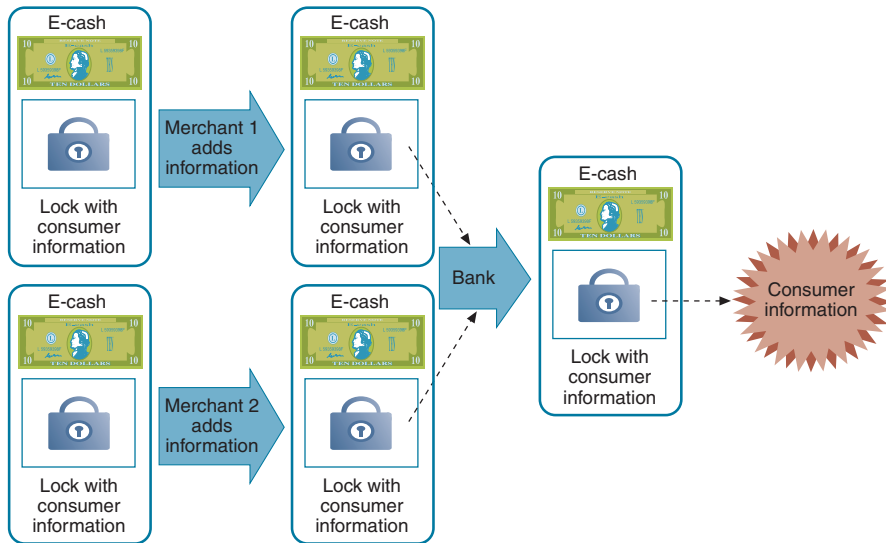


FIGURE 11-4 Detecting double spending of electronic cash

a situation—the consumer or the merchant. Of course, electronic cash that contains serial numbers is no longer anonymous, and anonymity is one reason to acquire electronic cash in the first place. Electronic cash containing serial numbers also raises a number of privacy issues, because merchants could use the serial numbers to track spending habits of consumers.

Creating truly anonymous electronic cash requires a bank to issue electronic cash with embedded serial numbers such that the bank can digitally sign the electronic cash while removing any association of the cash with a particular customer. The process begins when a consumer creates a random serial number that he or she sends to the bank issuing the electronic cash. The bank uses the consumer's random serial number along with the bank's digital signature and sends the random number, electronic cash, and digital signature as one package back to the user. When the user receives the electronic cash bundle, the user extracts the original random serial number and keeps the bank's digital signature. The consumer can now spend the electronic cash, which is digitally signed by the bank. When the consumer spends the electronic cash and the merchant passes it along to the issuing bank, the bank validates the electronic cash because it contains the bank's digital signature. However, the bank cannot determine the identity of the spender. It only knows that the electronic cash is genuine.

Electronic Cash Systems

Electronic cash has not been nearly as successful in the United States as it has been in Europe and Japan. In the United States, most consumers have credit cards, debit cards, charge cards, and checking accounts. These payment alternatives work well for U.S. consumers in both online and offline transactions. In most other countries of the world, consumers overwhelmingly prefer to use cash. Because cash does not work well for online

transactions, electronic cash fills an important need for consumers in those countries as they conduct B2C electronic commerce. This type of need does not exist in the United States because U.S. consumers already use payment cards for traditional commerce, and these payment cards work well for electronic commerce.

KDD Communications (KCOM) is the Internet subsidiary of Kokusai Denshin Denwa, which is Japan's largest global phone company. KCOM has its own NetCoin electronic cash system and offers electronic cash through its NetCoin Center. Shoppers can go to the NetCoin Center and obtain electronic cash that can be stored on their computers. Then, they can shop online for recipes or travel directories, or download MP3 music for less than a dollar per song. Other content providers, such as Japanese newspapers, provide access to their newspaper archives and charge a small fee to retrieve articles. Japan even has a donation site where visitors can donate electronic coins to charitable organizations.

Specific reasons for past failures of electronic cash systems in the United States are not completely clear. Some industry observers blame the failure on the way that many electronic cash systems were implemented. Most of these systems required the user to download and install complicated client-side software that ran in conjunction with the browser. Also, there were a number of competing technologies; therefore, no standards were ever developed for the entire electronic cash system. The absence of electronic cash standards means that consumers are faced with choosing from an array of proprietary electronic cash alternatives—none of which are interoperable. **Interoperable software** runs transparently on a variety of hardware configurations and on different software systems.

Despite their rough start, not all electronic cash ventures have failed. Next, you will learn about some of the Internet companies that currently offer electronic cash services and bill presentment and payment systems.

CheckFree

CheckFree, the largest online bill processor in the world, provides online payment processing services to both large corporations and individual Internet users. CheckFree provides infrastructure and software that permits users to pay all their bills with online electronic checks. CheckFree provides part of the technology that the Web portal Yahoo! uses to provide its **Yahoo! Bill Pay** service (see Figure 11-5).

Yahoo! Bill Pay service uses CheckFree transaction processing

YAHOO! FINANCE Finance Home - Yahoo! - Help

TRANSACTIONS GUARANTEED BY **CheckFree**

Welcome to Yahoo! Bill Pay

[Already enrolled?](#)

Getting Started

Step 1: Secure sign in.

Sign in using your Yahoo! ID and your Yahoo! [Security Key](#). If you don't have them, you can get them instantly.

Step 2: Enrollment.

Have your Driver's License, Social Security Number and checkbook handy.

Step 3: Start paying bills!

Pay any company or individual in the United States.

Security

Yahoo! Bill Pay uses your Yahoo! [Security Key](#).

Data transmitted securely via SSL encryption.

For information on your privacy, check out our [Privacy Information](#).



- **pay bills** anytime, anywhere for **FREE!**
- **schedule payments:** automatically or manually (get email reminders)
- **save money** on stamps, envelopes, & late fees

▶ **get started now!**

Premium Plan: • **Pay anyone**, anytime - in one convenient place
• Save money on stamps, envelopes, and late fees
• Receive bills electronically from over [200 billers](#)
• Your payments will be made on the date you set
• **First three months are FREE** - then just \$4.95/mo
*Includes 12 payments/mo (40¢ for each additional payment)

Basic Plan: • Make unlimited payments to over [100 billers](#)
• Receive bills electronically from over 85 billers
• Try it for free!

[Get Started Now!](#)

Need more information? [Take a Tour](#)

Copyright © 2004 Yahoo! Inc. All rights reserved. [Terms of Service](#)
[Privacy Information](#) - [Copyright Policy](#)
(for users of Yahoo! financial products and services)

FIGURE 11-5 Yahoo! Bill Pay service

Clickshare

Clickshare is an electronic cash system aimed at magazine and newspaper publishers. Clickshare's technology has occasionally been called a micropayment-only system; however, the ability to make micropayments is only one of Clickshare's features. Users with an ISP that supports Clickshare are registered automatically with Clickshare. When users click links leading to other sites that are registered with Clickshare, they can make purchases on those sites without having to register again. Clickshare keeps track of transactions and bills the user's ISP. The ISP, which already has an account relationship with the user, then bills the user for his or her purchases.

nother feature of Clickshare is that it tracks where a user travels on the Internet. This feature has significant value to advertisers and marketers that want to measure audience preferences; however, it does defeat anonymity, and anonymity is one reason that consumers might want to use Clickshare. The micropayment capability is, according to the company, a by-product of the core functionality of tracking identified users. Clickshare tracks users with the standard HTTP Web protocol and does not require cookies or software wallets. Clickshare claims to be the only company that can do this. (Click the **How Clickshare Works** link in the Online Companion for a diagram and explanation of how users are billed for the hyperlinks that they click.)

PayPal

PayPal is the electronic cash payment system that you read about in the opening case of this chapter. PayPal was founded in 1999, and in 2000 it merged with another payment processing service, X.com. PayPal provides payment processing services to businesses and to individuals. PayPal earns a profit on the **float**, which is money that is deposited in PayPal accounts and not used immediately. After two years in business, PayPal began charging a transaction fee to businesses that use the service to collect payments. Individuals who use PayPal to send money to other individuals do not pay a transaction fee. The free payment clearing service that PayPal provides to individuals is called a **peer-to-peer (P2P) payment system** because the payments are from one type of entity to another of the same type.

PayPal eliminates the need to pay for online purchases by writing and mailing checks or using payment cards. PayPal allows consumers to send money instantly and securely to anyone with an e-mail address, including an online merchant. PayPal is a convenient way for auction bidders to pay for their purchases, and sellers like it because it eliminates the risks posed by other types of online payments. PayPal transactions clear instantly so that the sender's account is reduced and the receiver's account is credited when the transaction occurs. Anyone with a PayPal account—online merchants or eBay auction participants alike—can withdraw cash from their PayPal accounts at any time by requesting that PayPal send them a check or make a direct deposit to their checking accounts. Figure 11-6 shows PayPal's home page.

To use PayPal, merchants and consumers first must register for a PayPal account. There is no minimum amount that a PayPal account must contain, and customers add money to their PayPal accounts by authorizing a transfer from their checking accounts or by using a credit card. Once members' payments are approved and deposited into their PayPal accounts, they can use their PayPal money to pay for purchases.

Merchants must have PayPal accounts to accept PayPal payments. Using PayPal to pay for auction purchases is very popular. A consumer can use PayPal to pay a seller for purchases even if the seller does not have a PayPal account. PayPal sends the seller an e-mail message indicating that a payment is waiting at the PayPal Web site. To collect PayPal cash, the seller or merchant that received the e-mail message must register and provide PayPal with payment instructions. PayPal then either sends the merchant a check or deposits funds directly into the merchant's checking account.

PayPal grew rapidly by serving the needs of buyers and sellers on auction sites such as eBay, Yahoo! Auctions, and Amazon Auctions. This success and its potential for profits did not go unnoticed by the management team at eBay. In May 1999, eBay purchased a

PayPal

[Sign Up](#) | [Log In](#) | [Help](#)

Welcome | Send Money | Request Money | Merchant Tools | Auction Tools

Member Log-In [Forgot your email address?](#)
[Forgot your password?](#)

Email Address

Password

Join PayPal Today
Now Over 86.6 million accounts

[Learn more about PayPal Worldwide](#)

Shop Without Sharing
Your Financial Information
PayPal. Privacy is built in. [Learn more](#)

How PayPal works. [Learn more](#)

16 Ways to Promote Your E-Business
[Download](#) your free guide today

Enterprise Solutions [Learn more](#)

What's New
[16 Ways to Promote Your E-Business](#)
[Protect your identity and more with OnGuard Online](#)

Buyers
[Send money](#) to anyone with an email address in 56 countries and regions.
PayPal is [free for buyers](#).
Shop without sharing [financial information](#).
[100% protection](#) against unauthorized payments sent from your account.

eBay Sellers
[Free eBay tools](#) make selling easier.
PayPal works hard to help [protect sellers](#).
PayPal simplifies [shipping and tracking](#).
[Earn cash back](#) with PayPal Preferred Rewards.

Merchants
[Accept credit cards](#) on your website using PayPal.
[Compare our solutions](#) to merchant accounts and gateways.
[Low fees](#) make PayPal the affordable choice.
Learn why PayPal is [good for business](#).

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [User Agreement](#) | [Developers](#) | [Jobs](#) | [Buyer Credit](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

— **PayPal, an eBay company**

Copyright © 1999-2005 PayPal. All rights reserved.
[Information about FDIC pass-through insurance](#)

identification as a part of eBay

FIGURE 11-6 PayPal home page

small electronic payments company and, one year later, sold a 35 percent stake in that company to Wells Fargo bank. This company, Billpoint, was operated as a joint venture between eBay and Wells Fargo. Billpoint grew rapidly, but PayPal maintained its first-mover advantage and remained the most widely used payment processing system on eBay. After unsuccessfully battling PayPal with its Billpoint service for three years, eBay finally gave up and decided to buy PayPal, as you learned in this chapter's opening case.

Other companies have entered the peer-to-peer payments business as well. First Data Corporation, which owns Western Union, offers what it calls electronic money orders that customers can use to settle auction transactions through its **BidPay** site. Traditional banks have also created Internet payment sites, such as Citibank's c2it payments service, but these have been less successful than nonbank entries into the business. In 2003, Citibank closed its c2it operation. Citibank does allow its customers to make peer-to-peer transfers from their checking accounts; however, that service requires the customer initiating the transfer to have a checking account with the bank.

ELECTRONIC WALLETS

As consumers are becoming more enthusiastic about online shopping, they have begun to tire of repeatedly entering detailed shipping and payment information each time they make online purchases. Filling out forms ranks high on online customers' lists of gripes about online shopping. To address these concerns, many electronic commerce sites include a feature that allows a customer to store name, address, and credit card information on the site. However, consumers must enter their information at each site with which they want to do business. An **electronic wallet** (sometimes called an **e-wallet**), serving a function similar to a physical wallet, holds credit card numbers, electronic cash, owner identification, and owner contact information and provides that information at an electronic commerce site's checkout counter. Electronic wallets give consumers the benefit of entering their information just once, instead of having to enter their information at every site with which they want to do business.

Electronic wallets make shopping more efficient. When consumers select items to purchase, they can then click their electronic wallet to order the items quickly. In the future, wallets could serve their owners by tracking purchases and maintaining receipts for those purchases. Maintaining records of a consumer's purchasing habits is something that online giants such as Amazon.com have mastered, but an enhanced digital wallet could reverse that process and use a Web robot to suggest where the consumer might find a lower price on an item that he or she purchases regularly.

Electronic wallets fall into two categories based on where they are stored. A **server-side electronic wallet** stores a customer's information on a remote server belonging to a particular merchant or wallet publisher. The main weakness of server-side electronic wallets is that a security breach could reveal thousands of users' personal information—including credit card numbers—to unauthorized parties. Typically, server-side electronic wallets employ strong security measures that minimize the possibility of unauthorized disclosure.

A **client-side electronic wallet** stores a consumer's information on his or her own computer. Many of the early electronic wallets were client-side wallets that required users to download the wallet software. This need to download software onto every computer used to make purchases is a chief disadvantage of client-side wallets. Server-side wallets, on the other hand, remain on a server and thus require no download time or installation on a user's computer. Before a consumer can use a server-side wallet on a particular merchant's site, the merchant must enable that specific wallet. Each wallet vendor must convince a large number of merchants to enable its wallet before it will be accepted by consumers. Thus, only a few server-side wallet vendors will be able to succeed in the market.

A disadvantage of client-side wallets is that they are not portable. For example, a client-side wallet is not available when a purchase is made from a computer other than the computer on which the wallet resides.

In a client-side electronic wallet, the sensitive information (such as credit card numbers) is stored on the user's computer instead of the wallet provider's central server. This removes the risk that an attack on a client-side electronic wallet vendor's server could reveal the sensitive information. However, an attack on the user's computer could yield that

information. Most security analysts agree that storing sensitive information on client computers is safer than storing that information on the vendor server because it requires attackers to launch many attacks on user computers, which are more difficult to identify (even though the user computers are less likely than a vendor server to have strong security features installed). It also prevents the easily identified servers of the wallet vendors from being attractive targets for such attacks.

For a wallet to be useful at many online sites, it should be able to populate the data fields in any merchant's forms at any site that the consumer visits. This accessibility means that the electronic wallet manufacturer and merchants from many sites must coordinate their efforts so that a wallet can recognize what consumer information goes into each field of a given merchant's forms.

Electronic wallets store shipping and billing information, including a consumer's first and last names, street address, city, state, country, and postal code. Most electronic wallets also can hold many credit card names and numbers, affording the consumer a choice of credit cards at the online checkout. Some electronic wallets also hold electronic cash from various providers.

A number of companies entered the electronic wallet business, including major firms such as MasterCard. Most of these companies have abandoned their efforts because current versions of all major browsers now include a feature that remembers names, addresses, and other commonly requested information and provides a one-click completion of fields on Web forms that request that information. Two survivors in the e-wallet arena are Microsoft .NET Passport and Yahoo! Wallet.

Microsoft .NET Passport

Microsoft .NET Passport (often referred to as Passport or Microsoft Passport) is a server-side electronic wallet operated by Microsoft. Anyone who obtains a Hotmail account, which is Microsoft's free e-mail service, is signed up automatically for a Passport account. People who use Microsoft MSN Internet access service also must sign up for a Passport account. Passport functions in the same way as most other electronic wallets—by completing order forms automatically. All of the personal data entered into a Passport wallet is encrypted and password protected.

Passport consists of four integrated services: Passport single sign-in service (SSI), Passport Wallet service, Kids Passport service, and public profiles. The sign-in service allows a user to sign in at a participating Web site using his or her username and password. The Passport Wallet service provides standard electronic wallet functions, such as secure storage and form completion of credit card and address information. When requested by a participating merchant, a consumer's secure information is released to the merchant so that the consumer does not need to enter data into a form. The Kids Passport service helps parents protect and control their children's online privacy, and the public profiles service allows consumers to create a public page of information about themselves.

Yahoo! Wallet

Yahoo! Wallet is a server-side electronic wallet offered by the Web portal site Yahoo! The Yahoo! Wallet functions in the same way as most other electronic wallets—by completing order forms automatically with identifying information and credit card payment

information. Yahoo! Wallet lets users store information about several major credit and charge cards, along with Visa and MasterCard debit cards.

Yahoo! Wallet is accepted by thousands of Yahoo! Store merchants (these are merchants on the Yahoo! Shopping section of the portal), and also can be used to pay for airplane tickets and hotel reservations booked through the Yahoo! Travel section of the portal. Yahoo! Wallet also works when users pay for premium services at Yahoo!, such as extra mail storage or Web hosting fees on the Yahoo! GeoCities Plus or Website Services portions of the site. Sellers on Yahoo! Auctions can pay their auction fees using the Yahoo! Wallet, too.

Yahoo! has the advantage of hosting a number of services and shops that it can be certain accommodate its own wallet; thus, it is certain to have a large number of merchants (including itself) that accept its wallet.

Many industry observers and privacy rights activist groups are concerned about electronic wallets because they give the company that issues the electronic wallet access to a great deal of information about the individual using the wallet. Several groups have attempted to enact standards intended to address wallet privacy concerns.

W3C Micropayment Standards Development Activity

Wallet information includes identification of the users and a complete record of their online purchasing activity. An alternative to having individual companies offer electronic wallet services is to have standards for electronic wallets built into the structure of the Web itself. With open standards, many different companies could offer electronic wallet services that would work on many different Web sites. This approach would distribute the information gathering and storage among a number of companies and thus reduce the risk of having one company in control of so much private information.

The World Wide Web Consortium (W3C) conducted an active standards development activity for micropayments in electronic commerce for several years. Although the activity has now been closed, the **W3C Electronic Commerce Interest Group (ECIG)** developed a set of standards called the **Common Markup for Micropayment Per-Fee-Links** before it ended its activities. This standard is a set of guidelines that provides an extensible and interoperable way to embed micropayment information in a Web page. An **extensible system** is one that developers can add to (or extend) without voiding any earlier work on the system. Although the ECIG standard showed promise, it was not adopted by a sufficient number of merchants and payment system operators to become successful.

The ECML Standard

The W3C initiative was not the only attempt to develop standards for the operation of electronic wallets. A consortium of several high-tech companies and credit card companies proposed an alternative standard that would replace the competing electronic wallet standards with a single standard. The consortium of companies, which includes America Online, Compaq, Dell, IBM, Microsoft, Visa U.S.A., and MasterCard, agreed on a set of XML tags called **ECML**, or **Electronic Commerce Modeling Language**. However, ECML has also failed to catch on among companies that create and use electronic wallets.

Assuming that an acceptable standard will evolve, the ultimate success of electronic wallets will depend on the confidence that Internet users have in the technology. As the NetBank story (see the Learning from Failures feature) illustrates, customer confidence is an important part of the success of any Internet technology, especially when that technology controls a person's financial welfare.

LEARNING FROM FAILURES

NetBank

CompuBank and NetBank were two of the first Internet banks to open in the United States. They were both pure Internet banks; that is, neither was founded by an existing bank with a physical presence. After four years of operation, CompuBank had about 50,000 accounts and \$64 million of deposits and was losing more than \$20 million per year. NetBank had done considerably better, with 160,000 accounts and \$1 billion of deposits and 10 consecutive quarters of profitability.

In early 2001, CompuBank decided to close its operations and found NetBank to be a willing purchaser of its accounts. When a bank buys accounts from another bank, it performs a series of procedures called due diligence. These **due diligence** procedures include checking the new customers' credit histories and banking records. Due diligence is usually performed before the transaction is completed and before the closing bank's customers look to the buying bank as the institution that will handle their accounts.

For a number of reasons, not all of which are clear, the due diligence process was still under way on the date that the transfer of accounts was to take place. NetBank placed holds on many accounts and sent letters to many account holders explaining that they were not acceptable customers by NetBank standards. For any bank, this would have been a difficult situation, but the nature of the two banks as Internet-only operations made things considerably worse for everyone.

Press accounts of the fiasco included stories of the problems that between 4000 and 8000 CompuBank depositors experienced. Some of the problems were small—online bill payments did not occur, debit and credit cards were rejected at stores and restaurants, and ATMs would not yield cash—while others were much larger. One couple who had kept the money to cover closing costs on a house purchase in a CompuBank account found that NetBank had placed a hold on the money.

Because they could not pay the closing costs, they were forced to find another mortgage lender. In the suit they filed against NetBank, the couple asserted that the increased rate on the mortgage loan would cost them tens of thousands of dollars. Other CompuBank customers were irritated that they lost access to their money for weeks. Some customers could not determine whether the bills they had set up to be paid automatically had, in fact, been paid.

continued

NetBank admitted failures in customer service related to the incident. Many customers who called to complain or ask for explanations experienced 45-minute waits on hold and then were transferred to the bank's Security Department, where a recording answered and asked callers to leave their Social Security numbers and wait to be called back. None of the customers reported being called back. The timing of NetBank's notification was problematic, too. Many customers reported receiving a letter from NetBank indicating that there were problems with their accounts. The letter, dated April 30, was received by the customers on or after May 14. The letter included a telephone number to call for assistance, but that number had been disconnected on May 12. Many of the unhappy customers found each other on Internet discussion boards and compared notes.

NetBank has not disclosed the number of customers it lost by its handling of this transition; indeed, it may not know. CompuBank's customers were largely experienced Internet users who chose to be part of the leading edge in handling their financial affairs. Many of them, after this experience, have sworn that they will never again do business with a bank that does not have a physical presence. The lesson from NetBank's experience is that customer service and the ability to communicate with customers become extremely important for companies that process electronic payments or are responsible for their customers' finances.

STORED-VALUE CARDS

Today, most people carry a number of plastic cards—credit cards, debit cards, charge cards, driver's license, health insurance card, employee or student identification card, and others. One solution that could reduce all those cards to a single plastic card is called a stored-value card.

A **stored-value card** can be an elaborate smart card with a microchip or a plastic card with a magnetic strip that records the currency balance. The main difference is that a smart card can store larger amounts of information and includes a processor chip on the card. The card readers needed for smart cards are different, too. Common stored-value cards include prepaid phone, copy, subway, and bus cards. Many people use the terms “stored-value card” and “smart card” interchangeably.

Magnetic Strip Cards

Most magnetic strip cards hold value that can be recharged by inserting them into the appropriate machines, inserting currency into the machine, and withdrawing the card; the card's strip stores the increased cash value. Magnetic strip cards are passive; that is, they cannot send or receive information, nor can they increment or decrement the value of cash stored on the card. The processing must be done on a device into which the card is inserted. Although both magnetic strip cards and smart cards can store electronic cash, a smart card is better suited for Internet payment transactions because it has some processing capability.

Smart Cards

A **smart card** is a stored-value card that is a plastic card with an embedded microchip that can store information. Credit, debit, and charge cards currently store limited information on a magnetic strip. A smart card can store about 100 times the amount of information that a magnetic strip plastic card can store. A smart card can hold private user data, such as financial facts, encryption keys, account information, credit card numbers, health insurance information, medical records, and so on.

Smart cards are safer than conventional credit cards because the information stored on a smart card is encrypted. For example, conventional credit cards show your account number on the face of the card and your signature on the back. The card number and a forged signature are all that a thief needs to purchase items and charge them against your card. With a smart card, credit theft is much more difficult because the key to unlock the encrypted information is a PIN; there is no visible number on the card that a thief can identify, nor is there a physical signature on the card that a thief can see and use as an example for a forgery.

Smart cards have been in use for more than a decade. Popular in Europe and parts of Asia, smart cards so far have not been as successful in the United States. In Europe and Japan, smart cards are being used for telephone calls at public phones and for television programs delivered by cable to people's homes. The cards are also very popular in Hong Kong, where many retail counters and restaurant cash registers have smart card readers. The city's transportation companies—subways, buses, railways, trams, and ferries—joined together and created a smart card called the Octopus that lets commuters use one card for all of their public transportation needs. The Octopus can be reloaded at any transportation location or at 7-Eleven stores throughout Hong Kong. The **Hong Kong Citybus** Web page with information about the Octopus Card appears in Figure 11-7.

Smart cards are beginning to appear in the United States. In San Francisco, the Bay Area **Metropolitan Transportation Commission** created a smart card system patterned after the Octopus Card. This system, TransLink, is the first integrated ticketing system for public transportation in the United States. The transportation smart card, implemented in a 2002 pilot program, allows commuters to ride most modes of public transit available in the city, including trains, buses, cabs, and ferries, by simply waving a single card near a reader device in transit vehicles or in stations. TransLink users can reload their smart cards at several retail outlets or directly from their bank accounts. The pilot program was a success and TransLink became available to all Bay Area transit customers in 2006.

Home | 繁體中文 | Text Only Version | Site Map | Links

Search site content here: GO

Bus Route Search | Airport Services | Octopus Card | Private Hire | Ocean Park | Hot Spots / Days Out

General Information | **Routes and Services** | News | How to Contact Us | Members Corner | Shop | FAQ

Traffic WebCam

Routes and Services | Octopus Card

Octopus Card

Introduction | Purchase & Travel | Adding Value | Fare Discounts

Octopus Card

Get on board with the Octopus
 Hong Kong public transport has a worldwide reputation for quality, efficiency and innovation. So when smart card technology was sufficiently developed, most of the major transport operators in Hong Kong formed a company to co-ordinate the design and purchase of a smart card ticketing system which would be used by all operators. For customer convenience the system uses only one ticket which is called the Octopus card.

Octopus is the "touch and go" electronic payment system. Each card contains a built-in microchip which contains the owner's payment information. You simply "beep" your Octopus card on a reader and the correct amount will be deducted from your card automatically. Octopus cards can be used in over 80 service providers in transport and non-transport sectors. For details, you can visit the [Octopus Cards Limited website](#).

Taking an Octopus on Citybus
 All Citybus buses are equipped with Octopus equipment and customers can now use their Octopus card for fare payment on all routes (except route 629 & 630). This means that you no longer need to carry loose change for your bus journeys, instead one ticket is all you need.

You can also enjoy several fare discounts by using Octopus Card when travelling on the designated routes, please visit [Fare Discount section](#) for details.

CITYBUS 城巴

Copyright (c) Citybus Limited, Hong Kong [2002]. All Rights Reserved. [Privacy Policy](#) [Terms of Use](#)

FIGURE 11-7 Octopus smart card information on the Hong Kong Citybus site

Visa introduced its smart card, the **smart Visa card**, in 2000. One of the first major promotions of the new Visa card occurred in late 2002 when retailer Target introduced its Target Visa smart card for use in Target stores and on the Target.com Web site. The Target Visa includes electronic wallet and automated login information for the Target.com Web site, but it also functions as a normal Visa card at other merchants. American Express has also released a smart card called **Blue**.

In the United States, the **Smart Card Alliance** advances the benefits of smart cards. The organization promotes the widespread acceptance of multiple-application smart card technology. Its members include companies in banking, financial services, computer technology, healthcare, telecommunications, and a number of government agencies. The Alliance focuses on information exchange and member interaction. Every member of the Alliance recognizes that smart cards can succeed in the United States only if a critical mass of smart cards supports applications—both physical and Internet-based—of interest to consumers. The Alliance promotes compatibility among smart cards, card reader devices, and applications.

INTERNET TECHNOLOGIES AND THE BANKING INDUSTRY

As you learned earlier in this chapter, the largest dollar volume of payments today are still made using paper checks. These paper checks are processed through the world's banking system. The other major payment forms in use today also involve banks in one way or another. This section outlines how Internet technologies are providing new tools and creating new threats for the banking industry.

Check Processing

In the past, checks were processed physically by banks and clearinghouses. When a person wrote a check to pay for an item at a retail store, the retailer would deposit the check in its bank account. The retailer's bank would then send the paper check to a clearinghouse, which would manage the transfer of funds from the consumer's bank to the retailer's account. The paper check would then be transported to the consumer's bank, which might then send the cancelled check to the consumer. In recent years, many banks have stopped sending cancelled checks to their consumer account holders to save postage. Despite these savings, the cost of transporting tons of paper checks around the country has grown each year.

In addition to the transportation costs, another disadvantage of using paper checks is the delay that occurs between the time that a person writes a check and the time that check clears the person's bank. This delay (which is similar to the delay you learned about earlier in PayPal accounts, and which is also called float) makes it possible to write checks a few days before money is in the account to cover those checks. In effect, the bank's customer obtains the free use of funds for a few days and the bank loses the use of those funds for the same time period. Although the delay normally lasts only a few days, there are times when it can become significantly longer. Railroad and airline strikes, for example, have caused the float to be extended. The most recent incidents that caused a significant increase in the float were the terrorist attacks of September 11, 2001.

Banks have been working for years to develop technologies that will help them reduce the float. In 2004, a U.S. law went into effect that many bankers believe will eventually eliminate the float. This law, called the **Check Clearing for the 21st Century Act** (or, more simply, **Check 21**), permits banks to eliminate the movement of physical checks entirely. In a Check 21-compliant world, the retailer can scan the customer's check. The scanned image is transmitted instantly through a clearing system and posts almost immediately to both accounts (that is, the withdrawal from the customer's account and the deposit to the retailer's account occur instantly), eliminating any float on the transaction.

You can learn more about the Check 21 law and its implementation by using the links in the Online Companion to the **BAI Check 21 Resource Center**, the **Federal Reserve Bank Check 21 Services** pages, or the **American Bankers Association Check 21 Resource Center**.

Phishing Attacks

In Chapter 10, you learned about the phishing expedition, which is a technique for committing fraud against the customers of online businesses. Although phishing expeditions can be launched against all types of online businesses, they are of particular concern to financial institutions because their customers expect a high degree of security to be maintained over the personal information and resources that they entrust to their online financial institutions.

The basic structure of a phishing attack is fairly simple. The attacker sends e-mail messages (such as the one shown in Figure 11-8) to a large number of recipients who might have an account at the targeted Web site (PayPal is the targeted site in the example shown in the figure). The e-mail message tells the recipient that his or her account has been compromised and it is necessary for the recipient to log in to the account to correct the matter. The e-mail message includes a link that appears to be a link to the login page of the Web site. However, the link actually leads the recipient to the phishing attack perpetrator's Web site, which is disguised to look like the targeted Web site. The unsuspecting recipient enters his or her login name and password, which the perpetrator captures and then uses to access the recipient's account. Once inside the victim's account, the perpetrator can access personal information, make purchases, or withdraw funds at will.

Date: [Date removed] 08:05:42 +0600
From: "Services PayPal" <services@paypal.com>
Subject: PayPal Account sensitive features are access limited!
To: [E-mail addresses removed]

Dear valued **PayPal** member:

PayPal is committed to maintaining a safe environment for its community of buyers and sellers. To protect the security of your account, PayPal employs some of the most advanced security systems in the world and our anti-fraud teams regularly screen the PayPal system for unusual activity.

Recently, our Account Review Team identified some unusual activity in your account. In accordance with PayPal's User Agreement and to ensure that your account has not been compromised, access to your account was limited. Your account access will remain limited until this issue has been resolved. This is a fraud prevention measure meant to ensure that your account is not compromised.

In order to secure your account and quickly restore full access, we may require some specific information from you for the following reason:

We would like to ensure that your account was not accessed by an unauthorized third party. Because protecting the security of your account is our primary concern, we have limited access to sensitive PayPal account features. We understand that this may be an inconvenience but please understand that this temporary limitation is for your protection.

Case ID Number: PP-040-187-541

We encourage you to log in and restore full access as soon as possible. Should access to your account remain limited for an extended period of time, it may result in further limitations on the use of your account.

However, failure to restore your records will result in account suspension. Please update your records within 48 hours. Once you have updated your account records, your **PayPal** session will not be interrupted and will continue as normal.

To update your **Paypal** records click on the following link:
<https://www.paypal.com/cgi-bin/webscr?cmd=login-run>

Thank you for your prompt attention to this matter. Please understand that this is a security measure meant to help protect you and your account. We apologize for any inconvenience.

Sincerely,
PayPal Account Review Department

PayPal Email ID PP522

Accounts Management As outlined in our User Agreement, **PayPal** will periodically send you information about site changes and enhancements.

Visit our Privacy Policy and User Agreement if you have any questions.
http://www.paypal.com/cgi-bin/webscr?cmd=p/gen/ua/policy_privacy-outside

FIGURE 11-8 Phishing e-mail message

The links in phishing e-mails are usually disguised. One common way to disguise the real URL is to use the “@” sign, which causes the Web server to ignore all characters that precede the “@” and only use the characters that follow it. For example, a link that displays:

```
https://paypal.com@218.36.41.188/fl/login.html
```

looks like it is an address at PayPal. However, the “@” sign causes the Web server to ignore the “paypal.com” and instead takes the victim to a Web page at the IP address “218.36.41.188.”

In the e-mail shown in the figure, the link appears in the victim’s e-mail client software as:

```
https://paypal.com/cgi-bin/webscr?cmd=_login-run
```

but when the victim clicks the link, the browser opens a completely different URL:

```
http://leasurelandscapes.com/snow/webscr.dll
```

Instead of the URL it shows in the e-mail client, the link in the phishing e-mail actually includes following JavaScript code:

```
<A onmouseover="window.status='https://www.paypal.com/cgi-bin/webscr?cmd=_login-run'; return true" onmouseout="window.status='https://www.paypal.com/cgi-bin/webscr?cmd=_login-run' "href="http://leasurelandscapes.com/snow/webscr.dll">https://www.paypal.com/cgi-bin/webscr?cmd=_login-run</A>
```

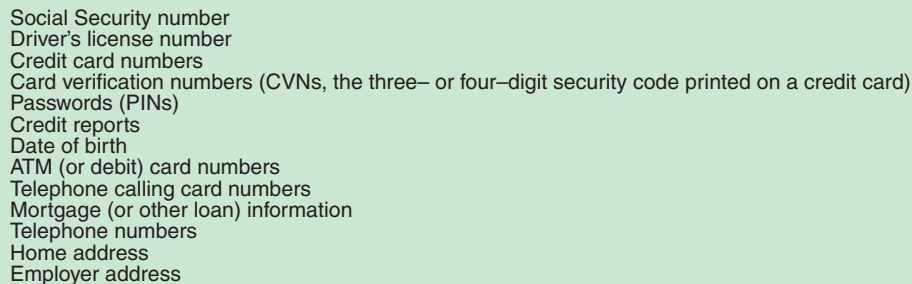
This code is invisible in many e-mail clients, so the victim might never know that the Web browser has opened a phony site. Phishing attack perpetrators use a variety of other tricks to hide the URLs, including code that pops up windows that look exactly like a browser address bar. The window is coded to pop up over the browser’s address bar. You can learn more about the details of phishing techniques by visiting the Web sites of the [Conferences on Email and Anti-Spam](#), and the [Anti-Phishing Working Group](#).

Organized Crime, Identity Theft, and Phishing Attacks

U.S. laws define **organized crime**, also called **racketeering**, as unlawful activities conducted by a highly organized, disciplined association for profit. The associations that engage in organized crime are often differentiated from less organized groups such as gangs and from organized groups that conduct unlawful activities for political purposes, such as terrorist organizations. Organized crime associations have traditionally engaged in criminal activities such as drug trafficking, gambling, money laundering, prostitution, pornography production and distribution, extortion, truck hijacking, fraud, theft, and insider trading. Often these activities are carried out simultaneously with legitimate business activities, which provide cover for the illegal activities.

The Internet has opened new opportunities for organized crime in their traditional types of criminal activities and in new areas such as generating spam (which you learned about in earlier chapters), phishing, and identity theft. **Identity theft** is a criminal act in

which the perpetrator gathers personal information about a victim and then uses that information to obtain credit. After establishing credit accounts, the perpetrator runs up charges on the accounts and then disappears. Figure 11-9 includes a list of the types of personal information that identity thieves most want to obtain (listed in approximate order of usefulness to the criminal).



- Social Security number
- Driver's license number
- Credit card numbers
- Card verification numbers (CVNs, the three- or four-digit security code printed on a credit card)
- Passwords (PINs)
- Credit reports
- Date of birth
- ATM (or debit) card numbers
- Telephone calling card numbers
- Mortgage (or other loan) information
- Telephone numbers
- Home address
- Employer address

FIGURE 11-9 Types of personal information most useful to identity thieves

Large criminal organizations can be highly efficient perpetrators of identity theft because they can exploit large amounts of personal information very quickly and efficiently. These organizations can use phishing attacks to gather personal information and then use it to perpetrate identity theft and other crimes. These criminal organizations often sell or trade information that they cannot use immediately to other organized crime entities around the world. Some of these criminal transactions are even conducted online. For example, a hacker who has planted zombie programs on a large number of computers (thus creating a **zombie farm**) might sell the right to use the zombie farm to an organized crime association that wants to launch a phishing attack (when a zombie farm is used this way, the attack is sometimes called a **pharming attack**). Individuals who commit these crimes have always posed a serious threat, but organized crime's entry into this activity increases the threat. There are two elements in phishing, the collection of the information (done by **collectors**) and the use of the information (done by **cashers**). The skills needed to perform these two activities are different. By facilitating transactions between collectors and cashers (and by participating as one or both), crime organizations have increased the efficiency and volume of phishing activity overall.

More than 2 million people fall victim to phishing attacks each year and experience financial losses exceeding \$900 million. Most experts believe that the percentage of online crime committed by organized crime associations will continue to increase in the future because it is so profitable.

Phishing Attack Countermeasures

In Chapter 8, you learned that several groups are working on ways to improve the Internet's mail transport protocols so that spam senders can be identified. Since spam is a key element of phishing attacks, any protocol change that improves e-mail recipients' ability to identify the source of an e-mail message will also help to reduce the threat of phishing attacks.

The most important step that companies can take today, however, is to educate their Web site users. Most online banking sites continually warn their customers that the site never sends e-mail that asks for account information or that asks the recipient to log in to their Web site and make changes to his or her account information. PayPal occasionally interrupts its own log-in screen sequence to insert a page that provides information about phishing attacks.

Many companies, especially those that operate financial Web sites, have contracted with consulting firms that specialize in anti-phishing work. These consultants monitor the Web for new Web sites that use the company's name or logo and move quickly to shut down those sites. Most phishing perpetrators set up their entrapping Web sites a few days before they launch their e-mail campaign, so this technique can be effective. Another anti-phishing technique is to monitor online chat rooms that are used by criminals. By watching for offers of stolen credit card information and other phishing exploits, consultants can identify phishing schemes that are under way.

The incidence of phishing attacks has grown rapidly over the past two years and most industry analysts expect that phishing will be a problem that will plague online businesses for the near future. Phishing can be an extremely profitable criminal activity and as more companies increase their defenses, analysts expect phishing perpetrators to become even better at working around those defenses.

Summary

Online stores can accept a variety of forms of payment. Credit, debit, and charge cards (payment cards) are the most popular forms of payment on the Internet. They are ubiquitous, convenient, and easy to use.

Electronic cash, one form of online payment, has been slow to catch on in the United States. A number of companies have faltered in recent years as they attempted to introduce electronic cash to the online world. Electronic cash is especially useful for making micropayments because the cost of processing payment cards for small transactions is greater than the profit on such transactions. Electronic cash shares several benefits with real cash: it is portable, anonymous, and usable for international transactions. Electronic cash can be stored online or offline. A third party, such as a bank, stores online electronic cash. The consumer holds offline cash in specially designed wallets.

Electronic wallets provide convenience to online shoppers because they hold payment card information, electronic cash, and personal consumer identification. Electronic wallets eliminate the need for consumers to reenter payment card and shipping information at a site's electronic checkout counter. Instead, the electronic wallet automatically fills in form information at sites that recognize the particular wallet software's technology. One persistent problem with electronic wallets is the lack of an internationally accepted standard. Both the W3C and the ECML standards group have created standards; however, neither has seen wide adoption by merchants, consumers, or wallet providers. With a single wallet standard, merchants would be more willing to install electronic, wallet-friendly software on their commerce sites.

Stored-value cards, including smart cards and magnetic strip cards, are physical devices that hold information, including cash value, for the cardholder. Magnetic strip cards have limited capacity. Smart cards can store greater amounts of data on a microchip embedded in the card and are intended to replace the collection of plastic cards people now carry, including payment cards, driver's licenses, and insurance cards. Trials of smart cards in a few U.S. cities have proved disappointing; however, smart cards are popular in other parts of the world. Visa and American Express have introduced smart cards. Unlike electronic cash or payment cards, smart cards require merchants to install new hardware that can read the smart cards.

Banks still process most monetary transactions, and a large part of the dollar volume of those transactions is still done by writing checks. Increasingly, banks are using Internet technologies to process those checks. Phishing expeditions and identity theft, especially when perpetrated by large criminal organizations, create a significant threat to online financial institutions and their customers. If not controlled, this threat could reduce the general level of confidence that consumers have in online business and hurt the growth of electronic commerce.

Key Terms

Acquiring bank	Charge card
Anonymous electronic cash	Chargeback
Automated Clearing House (ACH)	Check 21
Card not present transactions	Client-side electronic wallet
Casher	Closed loop system

Collector	Micropayments
Credit card	Money laundering
Credit card association	Open loop system
Customer issuing bank	Organized crime
Debit card	Payment card
Double-spending	Payment processing service provider
Due diligence	Peer-to-peer (P2P) payment system
Electronic cash	Pharming attack
Electronic Commerce Modeling Language (ECML)	Racketeering
Electronic wallet (e-wallet)	Scrip
EMV standard	Server-side electronic wallet
Extensible system	Single-use card
Float	Small payments
Identity theft	Smart card
Interoperable software	Stored-value card
Merchant account	Zombie farm
Merchant bank	

Review Questions

- RQ1. Write two paragraphs in which you define “scrip” and outline the advantages and disadvantages of scrip for consumers.
- RQ2. In about 100 words, describe the difficulties that can arise for merchants that want to process “card not present” credit card transactions.
- RQ3. In about 200 words, outline the reasons why a consumer who owns a credit card would want to use an electronic payment system, such as PayPal, for an Internet transaction. In an additional 200 words, outline the reasons that a small merchant might want to use an electronic payment system in addition to, or instead of, accepting credit cards.
- RQ4. In one paragraph, outline the problems that a company might encounter if it were to conduct international transactions using electronic cash.
- RQ5. In about 100 words, explain what electronic wallets are and how they can be useful to consumers.
- RQ6. In about 200 words, outline the advantages and disadvantages of smart cards for online merchants.

Exercises

- E1. Matt Remes has formed a small business and has just completed building an electronic commerce Web site that sells subscriptions to special-interest newsletters. The titles range from *Apple Growers Digest* to *Wilderness Backpacking Newsletter*. Many organizations and individuals produce the newsletters, and Matt’s role is to raise the visibility of these

somewhat obscure publications. The newsletters are published and available either biweekly or monthly. Unlike traditional subscription services, Matt's business has an agreement from all newsletter publishers that he can sell subscriptions for single issues or for periods of up to three years. He does not want to allow subscribers to use their payment cards to purchase a subscription that is less than two years in duration. But he finds that nearly 60 percent of the first-time customers on his site prefer to order a sample issue before committing to a subscription of a year or more. Discuss this case and present possible solutions to the problem. In about 200 words, describe existing systems that Matt could use to provide his subscribers with a system that does not depend on payment cards.

- E2. Bonnie Carson has owned and managed her gift and card shop in the Central Shopping Mall for three years. Business has been good, but Bonnie wanted to expand her business. One year ago, she hired a Web designer and built a Web site hosted by a national Internet service provider. Part of the monthly ISP fee for her merchant site includes the software needed to process credit card purchases. She has obtained a merchant account with a national credit card processing company. Bonnie's Web-based business is beginning to pick up. She wants to provide more payment options to her customers. Write a report in which you advise Bonnie on the use of payment processing services such as **PayPal**. Identify at least three reasons that Bonnie should use such a service and at least three reasons why she should not.
- E3. Evan Moskowitz has formed an Internet training company called Teach-U-Comp to market and sell computer courses online. The first courses the company will offer online are introductions to computer programming languages, including Visual Basic .NET, Java, and C++. Students can sign up for as many courses as they want, and each course takes four weeks to complete. Each course costs \$95, and students receive continuing education units (CEUs) based on the duration of the course and its level of difficulty. Evan is busy creating the online content and installing the course delivery software, and he hired you to investigate the feasibility of implementing an electronic wallet payment system in addition to the site's existing credit card payment system. Investigate available electronic wallet software, such as **Microsoft Passport** and **Gator**. You should also review the current status of the Electronic Commerce Modeling Language (**ECML**). Write a 400-word report of your findings for Evan. Conclude your report with specific recommendations.
- E4. During the Internet business expansion of the late 1990s, several major banks launched peer-to-peer payment systems. None of these systems was successful in competing with the PayPal system you learned about in this chapter. Two of the bank systems were Citibank's c2it and Bank One's eMoneyMail. In about 300 words, outline the reasons why you believe these two banks were unable to overcome PayPal's first-mover advantage. You can use your library, links in the Online Companion, and your favorite search engines to conduct your research.

C1. First Internet Bank of Indiana

During the first wave of electronic commerce, many established banks opened online branches and a considerable number of new, completely online, banks were formed. Many of these online banking initiatives were closed, sold, or merged into other operations after the first wave of electronic commerce had subsided. By 2001, many notable names that had dominated the first wave were gone. For example, Bank One had closed its online subsidiary Wingspan Bank and merged its operations into its existing retail banking department. Royal Bank of Canada had done the same thing with its Security First Network Bank (generally believed to have been the first online bank). CompuBank and G&L Internet Bank were both sold to other banks and USABancshares.com was closed in a flurry of fraud accusations and regulatory concerns.

Many of these early online banks faced similar challenges. They often bought loans instead of originating them. Purchased loans yield lower interest income because the originating bank always charges a fee or discount. They also tended to pay higher rates on customer deposits to attract new customers. These routes to rapid growth can significantly reduce profitability. Physical banks with many branches gain customers and market share because people walk or drive by a branch office and see the bank's name. Online banks must buy advertising that establishes them as viable brands in a highly competitive market. The need to purchase advertising also reduces profits. Small businesses were reluctant to deal with online banks in the early years of their existence. Small businesses generate considerable profits for banks because they tend to borrow money at relatively high interest rates and also tend to keep large balances in their checking accounts. Thus, there were a number of challenges that made survival difficult for online banks.

In 2004, the U.S. Federal Deposit Insurance Corporation (FDIC) issued a report on "limited-purpose banks" (which included Internet banks) in its *Future of Banking Study* series. The FDIC report concluded that the economics of operating an online bank were not attractive and that very few such banks could ever expect to be successful in the long term. The FDIC maintains an informal record of banks that operate primarily as Internet banks. That list recently included a meager 15 bank names. Of those 15, only three operate with no physical branch offices. One of those three is the **First Internet Bank of Indiana** (often called First IB).

First IB was launched in early 1999. By 2001, the bank had become profitable and had more than \$200 million in assets. Compared to the large international banks that dominate the industry, \$200 million is a relatively small amount (for example, the Bank of America has more than \$500 billion in assets), but First IB was able to operate efficiently and with low costs because it had no physical branch offices and very few employees compared to traditional banks.

First IB invested its resources in building the best Web site it could design and then followed a process of continually adjusting the site's design and the services offered to respond to customer comments and requests. For example, First IB created a frequently asked questions (FAQ) feature that reduced customer inquiries dramatically. It was also one of the first banks to offer statements and check images online. In 2004, the bank began to make check images available online the day after the check cleared (the industry average delay at that time was four to seven days). The bank has consistently received excellent reviews of its services by online business rating agencies and in the press.

Required:

1. Create a list of 10 specific concerns that a consumer might have when considering an online bank. Write a paragraph for each concern that describes how First IB addresses or fails to address it.
2. Evaluate how well the design of the First IB Web site meets the needs of a potential small business customer. In about 300 words, discuss the elements of the site that work particularly well in meeting the needs of this type of site visitor. In about 300 words, outline specific changes you would make to the site to better meet the needs of a potential small business customer.
3. Assume you are a security consultant hired by First IB. The president of the bank has become concerned about the potential damage that a phishing expedition directed at First IB customers could do to the bank's reputation. In about 500 words, analyze the phishing threat that faces First IB and outline steps that First IB should take to counter the threat.

Note: Your instructor might assign you to a group to complete this case, and might ask you to prepare a formal presentation of your results to your class.

C2. The Moose Hut

Rod and Martha Nelson started The Moose Hut (TMH), a gift shop in Calgary, Alberta, more than 15 years ago. The Nelsons have capitalized on the tourist trade drawn by the Calgary Stampede, which is one of the largest rodeos in the world. The shop sells a wide range of Canadian-themed items to rodeo fans and other tourists who visit central Alberta throughout the year. TMH's offerings range from inexpensive food items, such as pure Canadian maple syrup and smoked salmon, to much more expensive handcrafted gifts, including Inuit and First Nations artwork. The company's trademark product, the Moose Mug, is one of its biggest-selling items.

Many of TMH's customers return to the store whenever they visit Calgary. TMH's line of Canada Day Party Favours is especially popular with homesick Canadians who have moved to other countries, and TMH has been selling those products by mail order for the past several years. After reviewing the sales numbers for these mail order items, Martha has decided that it might be a good idea to expand the mail order operation and begin accepting orders through a Web site. Many of the store's items have a high value-to-weight ratio and would be easy to ship to customers around the world.

TMH currently accepts only checks denominated in Canadian or U.S. currency in its mail order operation; however, taking orders on a Web site will probably require the company to be more flexible in accepting multiple payment methods. Rod and Martha asked you to help them examine payment processing alternatives for TMH's new Web business.

To be acceptable, a payment processing method needs to handle all major credit cards, perform currency conversions, and be available to a Canadian merchant. Most important is that the payment processing method must be reasonably priced. The margins on most gift items at TMH are between 10 percent and 30 percent of the selling price, but the extra costs of shipping and handling items sold through the Web site will reduce those margins. TMH would like to keep the payment processing costs below 4 percent of the selling price, if possible.

Required:

1. Using the links in the Online Companion for this case, identify at least three payment processing options that might be suitable for TMH. Write a report of about three double-spaced pages in which you describe each of the three payment processing options. Include specific advantages and disadvantages for each option.
2. Prepare a one-page memorandum in which you make a specific recommendation to Rod and Martha. Include an explanation of the reasons for your recommendation.

Note: Your instructor might assign you to a group to complete this case, and might ask you to prepare a formal presentation of your results to your class.

For Further Study and Research

- American Banker*. 2002. "First Internet of Indiana Turns a Profit Again," 167(95), May 17, 13.
- Bach, D. 2001. "Web Stand-alone Model Gets a Lift," *American Banker*, 166(213), November 6, 1–2.
- Barlas, P. 2003. "PayPal Pushes for Business Use," *Investor's Business Daily*, October 24, A4.
- Bills, S. 2001. "Microsoft Says Aggregation on Site Doesn't Make It a Foe," *American Banker*, 166(167), August 29, 1–2.
- Boss, S., D. McGranahan, and A. Mehta. 2000. "Will the Banks Control Online Banking?" *The McKinsey Quarterly*, June, 70–77.
- Brandt, A. 2005. "Devious New Phishing Attack Outsmarts Typical Defenses," *PC World*, 23(3), March, 35.
- Card News*. 2003. "TouchCredit Founder Speaks Out On Biometrics And Online Payment Processing," 18(14), July 9, 1–2.
- Chakravorti, S. and T. McHugh. 2002. "Why Do We Use So Many Checks?" *Federal Reserve Bank of Chicago Economic Perspectives*, Third Quarter, 44–59.
- Credit Card Management*, 2003. "A Dubious Honor for Online Payments," 15(13), March, 14.
- CyberSource Corporation. 2005. *Sixth Annual Online Fraud Report: Online Payment Fraud Trends and Merchants' Response*. Mountain View, CA: CyberSource.
- Dragoon, A. 2004. "Fighting Phish, Fakes, and Frauds," *CIO Magazine*, 17(22), September 1, 33–38.
- Drake, C., J. Oliver, and E. Koontz. 2004. "Anatomy of a Phishing Email," *Proceedings of the First Conference on Email and Anti-spam*. Mountain View, CA, July 30.
- Dreazen, Y. 2002. "Money Transfers: Too User-Friendly? Legislation Aimed at Stopping Terrorism Could Have a Devastating Impact on an Innocent Bystander: PayPal," *The Wall Street Journal*, October 21, R9.
- Electronic Gaming Business*. 2003. "Micropayments Promise New Game Revenue Models," 1(8), July 30, 1–2.
- Financial Services Distribution*. 2004. "Specialist U.S. Banks: Internet Fails But Cards Shine," August 27, 11.
- Galbraith, J. 1995. *Money: Whence it Came, Where it Went*. London: Penguin Books.
- Gilbert, J. 2001. "Target's Use of Technology Boosts Its Brand Image," *Business 2.0*, June. (http://www.business2.com/marketing/2001/06/brand_technology.htm)
- Glasner, J. 2002. "Who'll Pay, Pal, for This IPO?" *Wired News*, February 5. (<http://www.wired.com/news/ebiz/0,1272,50220,00.html>)

- Grant, D. 2001. "Internet Banking Nightmare: Couple Sue After Access to Their Funds Was Cut Off for 10 Crucial Days," *EastSideJournal.com*, June 10. (<http://www.eastsidejournal.com/sited/story/html/56486>)
- Hammersley, B. 2003. "Online: Making the Web Pay," *The Guardian*, August 7, 24.
- Hisey, P. 2001. "Credit Card Fraud Hurts E-Tailers," *Retail Merchandiser*, 41(9), September, 33–34.
- Keizer, G. 2005. "Phishing Economics 101 Reveals Collectors and Cashers," *InternetWeek*, July 29. (<http://www.internetweek.com/showArticle.jhtml?articleId=166403894>)
- Kingston, J. 2001. "The Tech Scene: Don't Spend Your Last Flooz on Web Money," *American Banker*, 166(157), August 15, 1–2.
- Kingston, J. 2003. "E-Pay Overtaking Paper; Clients Want More Integration," *American Banker*, 168(81), April 29, 21.
- Krim, J. 2005. "More ID May Be Required for Online Banking," *The Washington Post*, October 21, D5.
- Kuykendall, L. 2003. "Citi to Pull the Plug on c2it Next Month," *American Banker*, October 1, 7.
- Lewis, H. 2001. "NetBank, CompuBank Merge, Customers Get Squashed," *Bankrate.com*, May 22. (<http://www.bankrate.com/bzrt/news/ob/20010521a.asp>)
- Magnusson, P. 2001. "Yes, They Certainly Will," *Business Week*, November 5, 90–91.
- Mantel, B. and T. McHugh. 2002. *Changing E-Payment Payment Networks in the U.S.: The Strategic, Competitive & Innovative Implications*. Chicago: Federal Reserve Bank of Chicago.
- Markoff, J. 2002. "Vulnerability Is Discovered in Security for Smart Cards," *The New York Times*, May 13. (<http://www.nytimes.com/2002/05/13/technology/13SMAR.html>)
- Marlin, S. 2003. "Who Needs Cash?" *Information Week*, December 29, 20–22.
- McHugh, T. 2002. "The Growth Of Person-To-Person Electronic Payments," *Chicago Fed Letter*, August, Number 180. (<http://www.chicagofed.org/publications/fedletter/2002/>)
- Mearian, L. 2005. "Wells Fargo Buys into Check Image Sharing," *Computerworld*, January 14. (<http://www.computerworld.com/databasetopics/data/story/0,10801,98966,00.html>)
- Miles, S. 2002. "What's a Check? After Years of False Starts, Online Banking Is Finally Catching On," *The Wall Street Journal*, October 21, R5.
- Mulligan, P. and S. Gordon. 2002. "The Impact of Information Technology on Customer and Supplier Relationships in the Financial Services," *International Journal of Service Industry Management*, 13(1), 29–46.
- Musgrove, M. 2005. "'Phishing' Keeps Luring Victims," *The Washington Post*, October 22, D1.
- Nahnybida, S. 2003. "Expectations Unfulfilled on E-Billing, E-Payments," *Bank Technology News*, 16(10), October, 62–63.
- Orr, B. 2002. "EPN Wants To Be the Payments Backbone of E-Commerce," *ABA Banking Journal*, 94(12), December, 52–54.
- Ptacek, M. 2001. "CompuBank's Demise May Signal a New Era," *American Banker*, 166(63), April 2, 16.
- Quain, J. 2003. "Can You Spare Some Change?" *PC Magazine*, 22(23), December 30, 25.
- Ramsaran, C. 2004. "Catch of the Day: Banks Face New Phishing Scams," *Bank Systems & Technology*, December 1, 13.
- Ramstad, E. 2004. "Hong Kong's Money Card Is a Hit," *The Wall Street Journal*, February 19, B3.
- Rist, C. 2003. "Making Bank on Small Change," *Business 2.0*, 4(10), November, 56–57.
- Rob, M. and E. Opara. 2003. "Online Credit Card Processing Models: Critical Issues to Consider by Small Merchants," *Human Systems Management*, 22(3), 133–142.
- Roberts-Witt, S. 2001. "Show Me the Money," *PC Magazine*, 20(6), March 20, 13–15.

- Robinson, B. 2001. "Is It Too Late for Smart Cards?" *Information Week*, March 19, 81–83.
- Rosato, D. 2004. "Why Are You Still Writing Checks?" *Money*, 33(1), January, 94–97.
- Roth, A. 2001. "CompuBank Merge Nettles NetBank," *American Banker*, 166(119), June 21, 1–2.
- Rush, L. 2003 "Get Paid: P2P Payments Gaining Consumer Trust," *E-Commerce Guide*, November 18. (http://ecommerce.internet.com/how/paid/article/0,10364_3110831,00.html)
- Scucka, D. 2001. "Charging Into Japan: eCharge Thinks Japan's Consumers Will Take to Its Net-Based System," *J@pan Inc*, 3(4), April, 70–72.
- Smith, G. 2002. "Account Aggregation Falls Apart," *Business Week*, July 2. (http://www.businessweek.com/technology/content/jul2002/tc2002072_3404.htm)
- Stoneman, B. 2003. "FAQs Lighten Service Load at First Internet Bank of Indiana," *American Banker*, 168(2), January 13, 12.
- Sturgeon, J. 2003. "Electronic Payments," *CFO Magazine*, 19(15), Winter, 52–53.
- Tedeschi, B. 2004. "Protect Your Identity," *PC World*, 22(12), December, 107–112.
- United States Census Bureau. 2004. *2004-2005 Statistical Abstract of the United States*. Washington, D.C.: U.S. Census Bureau.
- Urban, M. 2005. "To Catch Phish, Banks Need Better Bait," *Bank Technology News*, 18(11), November, 57.
- Wingfield, N. and J. Sapsford. 2002. "eBay to Buy PayPal for \$1.4 Billion," *The Wall Street Journal*, July 9, A6.
- Yom, C. 2004. "Limited-purpose Banks: Their Specialties, Performance, and Prospects," *FDIC Future of Banking Study Series*, June, 1–45. Washington, D.C.: Federal Deposit Insurance Corporation (FDIC).

