Chapter 11

Payments Systems For Electronic Commerce

At a Glance

Instructor’s Manual Table of Contents

Lecture Notes

Chapter Overview

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.

Chapter 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

Instructor Notes

Online Payment Basics

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.

Credit cards are by far the most popular form of consumer electronic payments online. 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 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, this turned out not to be true.

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.

Payment Cards:	♦ **Credit card:** 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. ♦ **Debit card:** Removes the amount of the sale from the cardholder’s bank account and transfers it to the seller’s bank account. ♦ **Charge card:** Carries no spending limit, and the entire amount charged to the card is due at the end of the billing period.

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 - called card not present transactions because the merchant’s location and the purchaser’s location are different - 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.

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 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).

Steps Followed by Payment Card Transactions:	♦ The merchant authenticates the payment card to ensure it is valid and not stolen. ♦ 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. ♦ Settlement occurs, usually a few days after the purchase, which means that funds travel between banks and are placed into the merchant's account.

Quick Quiz

1. _____ 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.
   Answer: Electronic cash

2. Internet payments for items costing from a few cents to approximately a dollar are called _____.
   Answer: micropayments

3. _____ is spending a particular piece of electronic cash twice by submitting the same electronic currency to two different vendors.
Answer: Double spending

4. _____ 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.
Answer: Money laundering

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.

Teaching Tip:	♦ Have students research Web sites that accept electronic cash and determine the type of organizations that accept this form of payment. Students should submit a brief report summarizing their findings.

Electronic Cash:	♦ **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. ♦ **Privacy and Security of Electronic Cash:** 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.

- **Holding Electronic Cash: Online and Offline Cash:** 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. 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.

Advantages and Disadvantages of 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.

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.

Providing Security for Electronic Cash

Cryptographic algorithms are the keys to creating tamper-proof 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 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.

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 if two deposits of the same electronic cash are about to occur, it is impossible to ascertain who is at fault in such 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.

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.

Electronic Cash Systems:	♦ **CheckFree:** The largest online bill processor in the world, provides online payment processing services to both large corporations and individual Internet users.

	♦ **Clickshare:** An electronic cash system aimed at magazine and newspaper publishers. ♦ **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.

Quick Quiz

1. Internet payments for items costing from a few cents to approximately a dollar are called _____.
   Answer: micropayments

2. True or False: Online cash storage is the virtual equivalent of money kept in a wallet.
   Answer: False

3. _____ 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.
   Answer: Money laundering

4. _____ is electronic cash that, like bills and coins, cannot be traced back to the person who spent it.
   Answer: Anonymous electronic cash

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' list 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 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 serverside 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.

Teaching Tip:	♦ Have students conduct research on the Web to determine the security implications of using an e-wallet.

Microsoft .NET Passport

Microsoft .NET Passport (often referred to as Passport or Microsoft Passport) is a serverside 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.

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

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 micro payment information in a Web page.

The ECML Standard

The W3C initiative is 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, has agreed on a technology called ECML, or Electronic Commerce Modeling Language. However, ECML has also failed to catch on among companies that create and use electronic wallets.

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.

Stored-Value Cards:	♦ **Magnetic strip card:** Holds a value that can be recharged by inserting it 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. ♦ **Smart card:** 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.

Issues Box: More smart card standards, please

A National Institute of Standards and Technology study found a need for additional technical and policy standards as agency officials discover more uses for smart cards spanning organizations. Smart cards are increasingly being used both for controlling physical access to government facilities and authenticating federal users' identities online.

The study found a need for better coordination among agency officials in setting policies on the types of personal information that can be stored on smart cards. A report on the study also states that consistent, government-wide policies are needed for who can enter and update personal information on the cards and how that should be done. The lack of consistent policies poses a barrier to interoperability.

The Defense Department, currently the largest federal user of smart cards, needs more consistent public-key infrastructure (PKI) policies so that users do not have to present unique PKI credentials at each of the facilities to which they need to gain access, the report states. DOD has issued 4 million smart cards so far.

Officials at the State Department, another potentially large user of smart card technology, also need to settle on a single technical standard that they can use for the agency's various government travel documents. Department officials currently favor so-called contactless smart card technology as the standard that can best accommodate State's needs, the study found. Contactless smart cards function at different ranges and frequencies and require no direct contact with readers.

The report concludes with recommendations that smart card policy or technical standards be developed for:

- Biometrics, card-to-reader authentication, physical access and PKI interoperability.
- Best practices and reference models.
- Government Smart Card Interoperability Specification options.
- Cross-agency credentialing.
- Migrating to newer technologies such as contactless cards.
- Integrating applications on a card.

Source: *http://www.fcw.com/fcw/articles/2004/0419/web-nist-04-23-04.asp*

Question

1. What are the advantages of developing technical standards?
2. Why do you think smart cards have not been as successful in the United States as they have been in Europe?

Internet Technologies and the Banking Industry

This section outlines how Internet technologies are providing new tools and creating new threats for the banking industry.

Check Processing

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.

Phishing Attacks

Phishing expeditions, a technique for committing fraud against the customers of online businesses, can be launched against all types of online businesses, but 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 to a large number of recipients who might have an account at the targeted Web site. 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.

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.

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.

Quick Quiz

1. A(n) _____ wallet stores a customer's information on a remote server belonging to a particular merchant or wallet publisher.
   Answer: server-side electronic

2. True or False: There are two elements in phishing, the collection of the information (done by collectors) and the use of the information (done by cashers).
   Answer: True

3. A(n) _____ can be an elaborate smart card with a microchip or a plastic card with a magnetic strip that records the currency balance.
   Answer: stored-value card

4. True or False: Smart cards are safer than conventional credit cards because the information stored on a smart card is encrypted.
   Answer: True

Discussion Questions

- Why is the idea of using electronic cash still so popular despite the many failures in the last few years?
- Why do you think micropayments have so far, not been implemented very well on the Web?

Additional Resources

- Smart Cards: http://www.howstuffworks.com/question332.htm
- Electronic Cash: http://www.rsasecurity.com/rsalabs/node.asp?id=2285
- Microsoft Passport Network: http://en.wikipedia.org/wiki/Microsoft_.NET_Passport

Key Terms

- **Acquiring bank:** Bank that does business with sellers (both Internet and non-Internet) that want to accept payment cards.
- **Chargeback:** The process that occurs when a cardholder successfully contests a charge and the merchant bank retrieves the money it placed in the merchant account.
- **Double-spending:** Spending a particular piece of electronic cash twice by submitting the same electronic currency to two different vendors.
- **Electronic cash:** 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.
- **Micropayments:** Internet payments for items costing from a few cents to approximately a dollar.
- **Money laundering:** 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.
- **Smart card:** A stored-value card that is a plastic card with an embedded microchip that can store information.