

E-Business Tenth Edition

Chapter 11 Online Payment Systems

Learning Objectives

In this chapter, you will learn:

- The basic functions of online payment systems
- How payment cards are used in electronic commerce
- About the history and future of electronic cash
- How digital wallets work
- What stored-value cards are and how they are used in electronic commerce
- How the banking industry uses Internet technologies

Online Payment Basics

- Online payments
 - Important electronic commerce site function
 - Several online payment options available
 - Vary in size and processing method

Micropayments and Small Payments

- **Micropayments**
 - Internet payments for items costing few cents to a dollar
- **Micropayments barriers**
 - Not yet implemented very well on the Web
 - Human psychology
 - People prefer to buy small value items in fixed price chunks
 - Example: mobile phone fixed monthly payment plans

Micropayments and Small Payments (cont'd.)

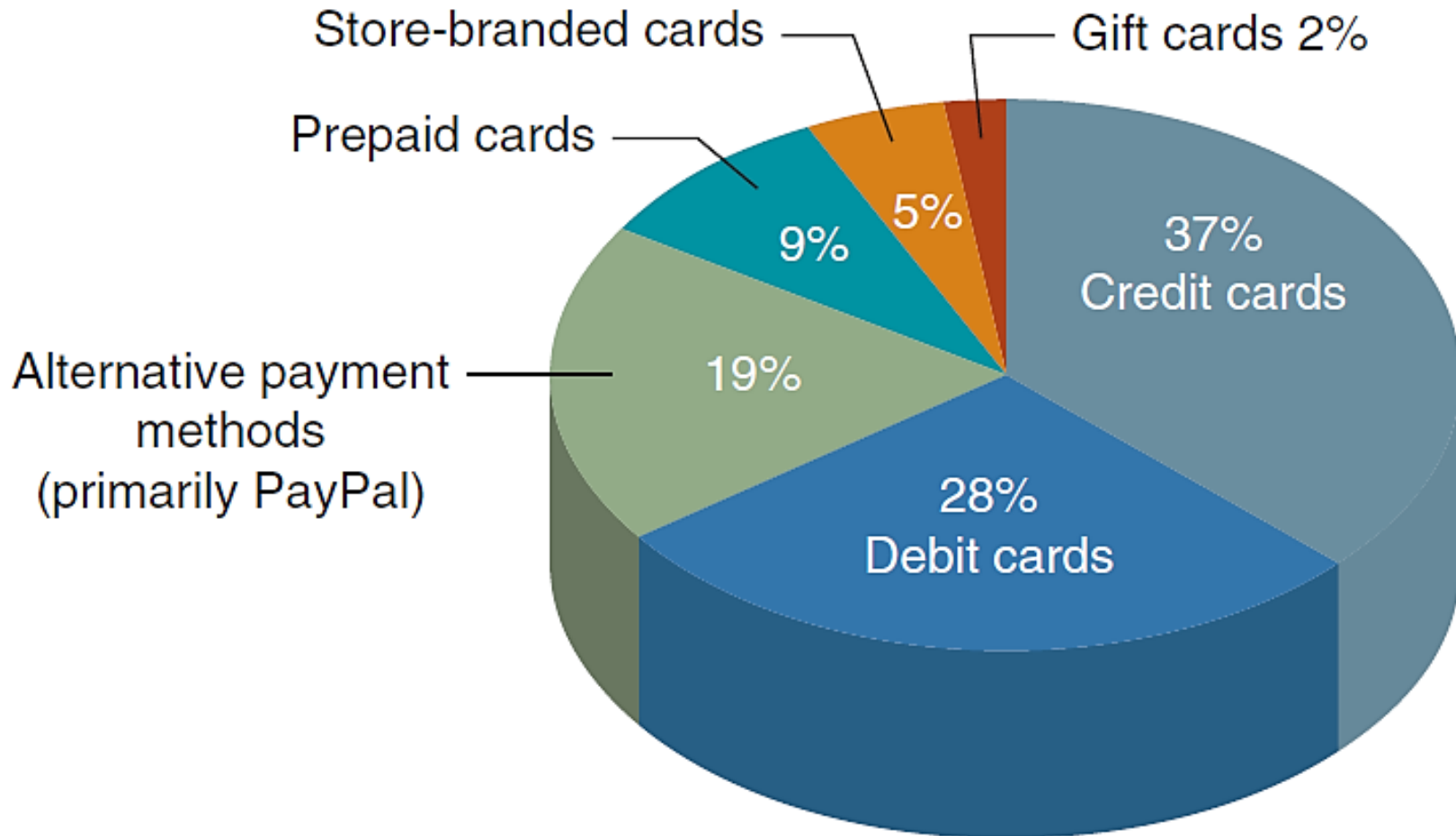
- Companies that have developed micropayment systems
 - Millicent, DigiCash, Yaga, BitPass
 - All failed
 - No company gained broad acceptance of its system
 - No company devoted solely to offering micropayment services

Micropayments and Small Payments (cont'd.)

- **Small payments**
 - All payments of less than \$10
 - Being offered through mobile telephone carrier
 - Buyers make purchases using their mobile phones
 - Charges appear on monthly mobile phone bill
 - Bright future held back by mobile carriers' substantial charges

Online Payment Methods

- Four ways to purchase items (traditional and electronic)
 - Cash, checks, credit cards, debit cards
 - 90% of all United States consumer payments
- Electronic transfer: small but growing segment
 - Popular example: automated payments
- Credit and debit cards
 - Worldwide: 85% of online payments
 - Remainder of payments primarily PayPal



Source: Adapted from forecasts by Javelin Strategy & Research and *Internet Retailer*.

FIGURE 11-1 Forms of payment for U.S. online transactions, estimates for 2015

E-Business, Tenth Edition

Online Payment Methods (cont'd.)

- Online payment systems
 - Still evolving
 - Competition for dominance
 - Cheaper than mailing paper checks
 - Convenient for customers
 - Save companies money
- Costs per bill
 - Billing by mail: between \$1.00 and \$1.50
 - Internet billing and payment costs: 50 cents
- Significant environmental impact

Online Payment Methods (cont'd.)

- Online business payment requirements
 - Safe, convenient, and widely accepted
- Determine which choices best for company and customers
- Each payment technology:
 - Unique properties, costs, advantages, and disadvantages

Payment Cards

- **Payment card**
 - Describes all types of plastic cards used to make purchases
 - Categories: credit cards, debit cards, charge cards, prepaid cards, and gift cards
- **Credit card (Visa, MasterCard)**
 - Spending limit based on user's credit history
 - Pay off entire credit card balance
 - May pay minimum amount
 - Card issuers charge unpaid balance interest
 - Widely accepted
 - Consumer protection: 30-day dispute period

Payment Cards (cont'd.)

- **Card not present transactions**
 - Cardholder not present during transaction
 - Extra degree of risk for merchant and bank
- **Debit card (electronic funds transfer at point of sale (EFTPOS) cards)**
 - Removes sales amount from cardholder's bank account
 - Transfers sales amount to seller's bank account
 - Issued by cardholder's bank
 - Carries major credit card issuer name

Payment Cards (cont'd.)

- **Charge card** (e.g., American Express)
 - No spending limit
 - Entire amount due at end of billing period
 - No line of credit or interest charges
 - Examples: department store, oil company cards
- Retailers may offer their own charge cards
 - **Store charge cards** or **store-branded cards**

Payment Cards (cont'd.)

- **Prepaid cards**
 - Cards that can be redeemed by anyone for future purchase
 - **Gift cards:** prepaid cards sold to be given as gift
- **Single-use cards**
 - Cards with disposable numbers
 - Addresses concern of giving online vendors payment card numbers
 - Valid for one transaction only
 - Designed to prevent unscrupulous vendor fraud
 - Withdrawn from market due to lack of consumer use

Advantages and Disadvantages of Payment Cards

- Advantage for merchants
 - Fraud protection
 - Can authenticate and authorize purchases using a payment card processing network
 - **Interchange network**: set of connections between credit card issuing banks, associations owning credit cards, and merchants' banks
- Advantage for U.S. consumers
 - Liability of fraudulent card use: \$50
 - Frequently waived if card stolen

Advantages and Disadvantages of Payment Cards (cont'd.)

- Greatest advantage
 - Worldwide acceptance
 - Currency conversion handled by card issuer
- Disadvantage for merchants
 - Per-transaction fees, monthly processing fees
 - Viewed as cost of doing business
 - Goods and services prices: slightly higher
 - Compared to environment free of payment cards
- Disadvantage for consumers
 - Annual fee

Advantages and Disadvantages of Payment Cards (cont'd.)

- Provide built-in security for merchants
 - Assurance of payments
- Card transaction steps transparent to consumers
- Entities involved in payment card processes:
 - Merchant, merchant's bank, customer, customer's bank, and payment card issuer (company)

Payment Acceptance and Processing

- Internet payment card process made easier
 - Due to standards
- United States online stores, mail order stores
 - Must ship merchandise within 30 days of charging payment
 - Significant violation penalties
 - Charge account when shipped

Payment Acceptance and Processing (cont'd.)

- Processing payment card transaction online
 - Payment acceptance
 - Establish card validity
 - Verify card's limit not exceeded by transaction
 - Clearing the transaction
 - All steps to move funds from card holder's bank account into merchant's bank account

Payment Acceptance and Processing (cont'd.)

- Open and closed loop systems
 - **Closed loop systems**
 - Card issuer pays merchant directly
 - Does not use intermediary
 - American Express, Discover Card
 - **Open loop systems** (three or more parties)
 - Additional payment processing intermediaries
 - Visa, MasterCard: not issued directly to consumers
 - **Credit card associations**: operated by association member banks
 - **Customer issuing banks (issuing banks)**: banks issuing cards

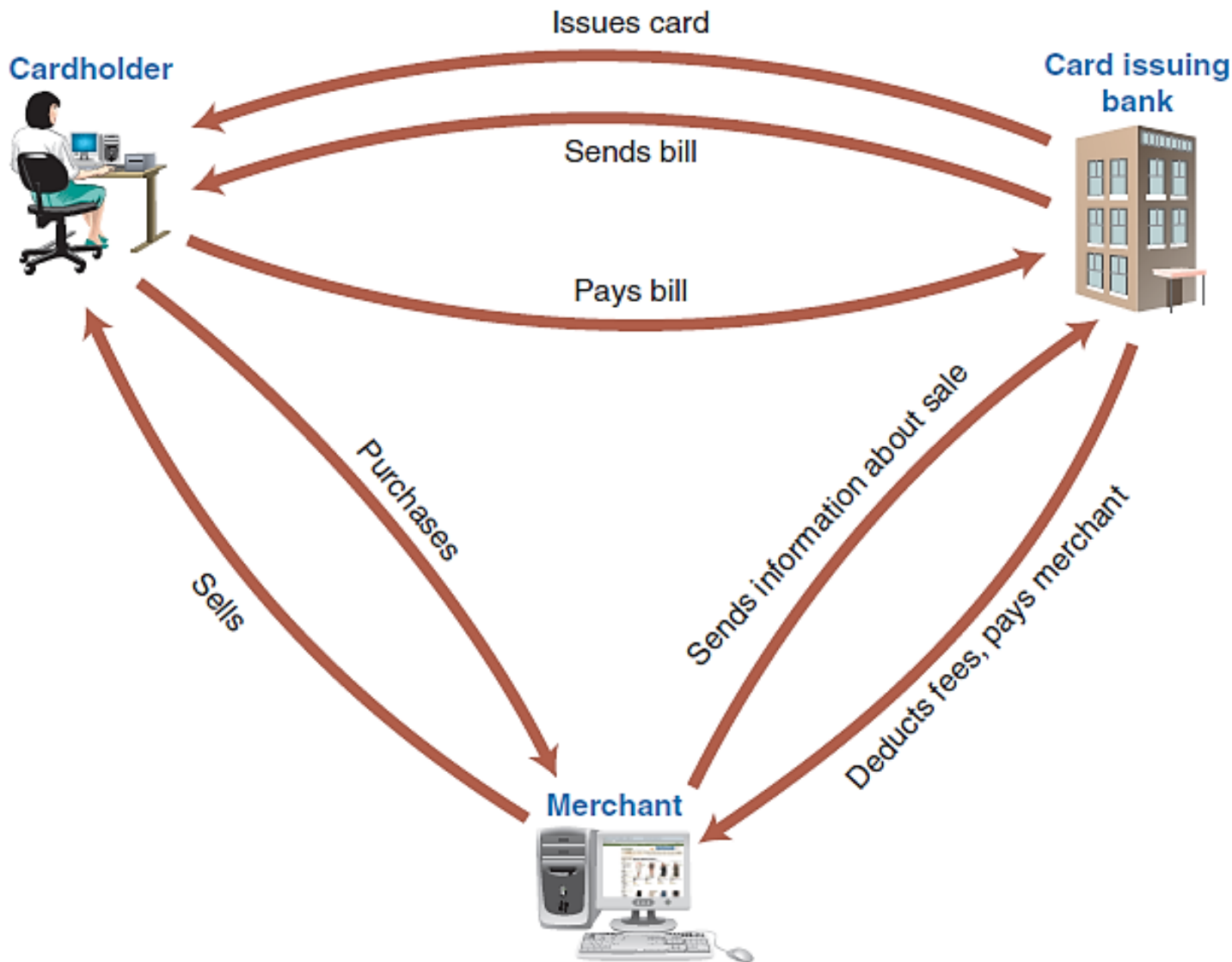


FIGURE 11-2 Closed loop payment card system

E-Business, Tenth Edition

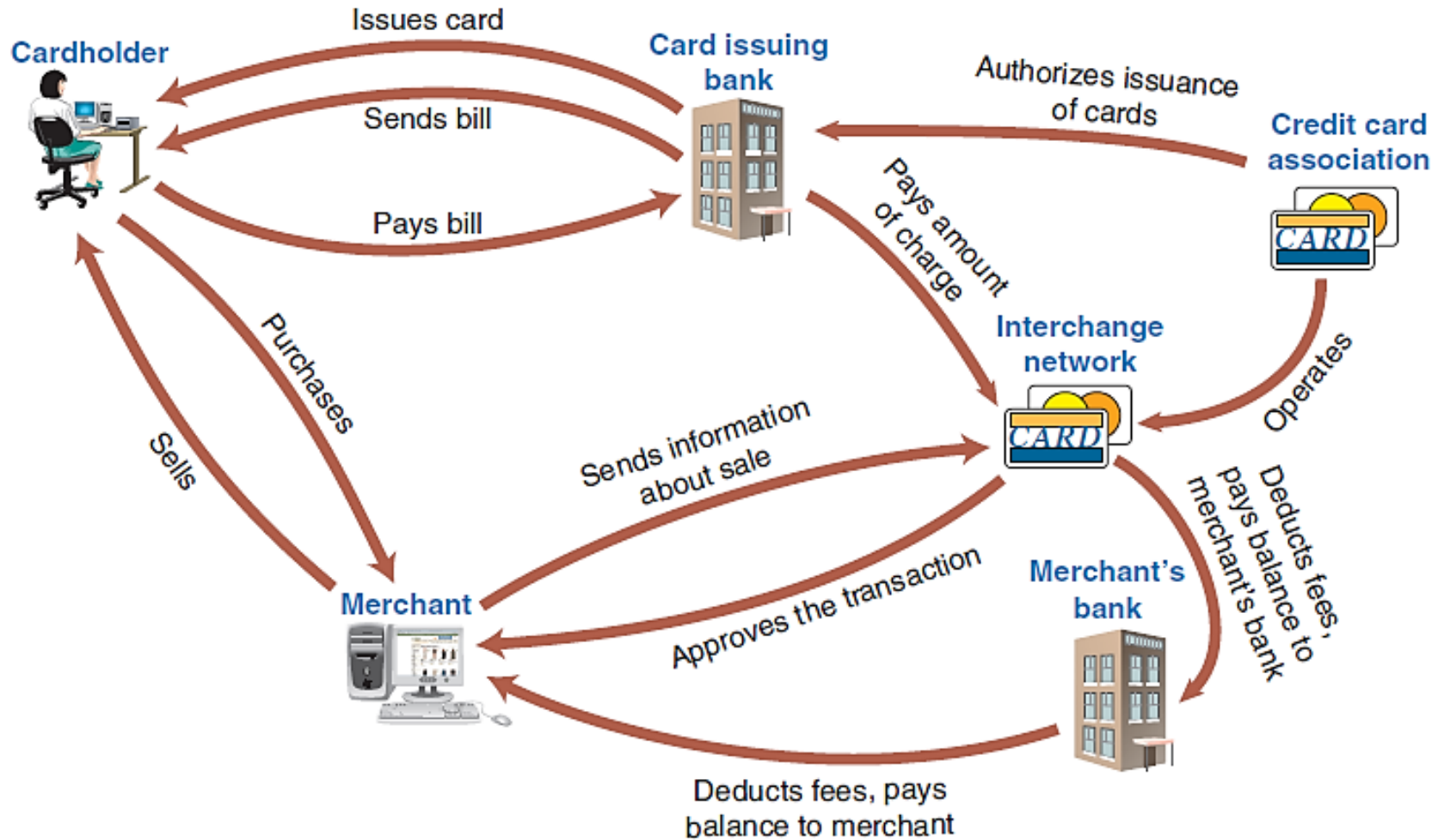


FIGURE 11-3 Open loop payment card system

Payment Acceptance and Processing (cont'd.)

- Merchant accounts
 - **Acquiring bank:**
 - Does business with Internet and non-Internet sellers
 - Wants to accept payment cards
 - **Merchant account** required by online merchant to process Internet transactions payment cards
 - Obtaining account
 - Merchant provides business information
 - Bank assesses business type risk
 - Bank assesses percentage of sales likely to be contested

Payment Acceptance and Processing (cont'd.)

- **Chargeback** process
 - Cardholder successfully contests charge
 - Merchant bank must retrieve money from merchant account
 - Merchant may have to keep funds on deposit
- Additional fees
 - **Acquirer fees:** charges for providing payment card processing service
 - **Interchange fees:** set by the card association, charged to acquiring bank, passed along to merchant

Payment Acceptance and Processing (cont'd.)

- Problem facing online businesses: fraud
 - Under 15 percent of all credit card transactions completed online
 - Responsible for 64 percent of total dollar amount of credit card fraud
- Online transaction fraud increased steadily through 2008
 - Slight decline since 2008

Payment Acceptance and Processing (cont'd.)

- Merchants' use of antifraud measures
 - Scoring services providing risk ratings for individual transactions in real time
 - Shipping only to card billing address
 - Requiring card verification numbers (CVNs) for card not present transactions
- **CVN**
 - Three- or four-digit number printed on the credit card
 - Not encoded in the card's magnetic strip

Payment Acceptance and Processing (cont'd.)

- Processing payment card transactions
 - Most online merchants have internal systems:
 - Handling closed loop and open loop system cards
 - Some accept direct deductions from customer's checking account
 - **Automated Clearing House (ACH):** network of banks involved in direct deduction transactions
 - Business size considerations
 - Large: entire department to build/maintain systems
 - Mid-size: purchased software with skilled staff to manage system
 - Small: rely on service provider

Payment Acceptance and Processing (cont'd.)

- **Payment processing service providers (payment processors)**
 - Companies offering payment card processing
- **Front-end processor (payment gateway):**
 - Obtains transaction authorization
 - Stores approval or denial record
- **Back-end processor:** takes front-end processor transactions and coordinates information flows
 - Handles chargebacks, other reconciliation items through the interchange network and acquiring and issuing banks, including ACH transfers

Payment Acceptance and Processing (cont'd.)

- Payment processors:
 - IPPay, Authorize.Net, Global Payments, and FirstData
- Specialized payment processing services:
 - Digital River's*shareit!
- Third party payment processor may be evident or transparent to customer
 - Well-recognized name provides customers with sense of security

Electronic Cash

- **Electronic cash** (e-cash, digital cash)
 - Describes any value storage and exchange system created by private (nongovernmental) entity
 - Does not use paper documents or coins
 - Can serve as substitute for government-issued physical currency
- **Potential market**
 - Purchases below \$10
 - Majority of world's population who do not have credit cards

Privacy and Security of Electronic Cash

- Electronic payment method concerns
 - Privacy and security, independence, portability, convenience
 - Privacy and security: most important to consumers
 - Vulnerable transactions
 - Electronic currency: copied, reused, forged
- Important characteristics of electronic cash
 - Ability to spend only once
 - Anonymous use
 - **Anonymous electronic cash:** can't be traced to person who spent it
 - Convenience

Holding Electronic Cash: Online and Offline Cash

- Online cash storage
 - Consumer has no personal possession of electronic cash
 - Trusted third party (online bank) involved in all transfers, holds consumers' cash accounts
- Online system payment
 - Merchants contact consumer's bank
 - Helps prevent fraud (confirm valid cash)
 - Resembles process of checking with consumer's bank to ensure valid credit card and matching name

Holding Electronic Cash: Online and Offline Cash (cont'd.)

- Offline cash storage
 - Virtual equivalent of money kept in wallet
 - Customer holds it
 - No third party involved in transaction
 - Protection against fraud concern
 - Hardware or software safeguards needed
 - **Double-spending**
 - Spending electronic cash twice
 - Submit same electronic currency to two different vendors
 - Not enough time to prevent fraudulent act

Holding Electronic Cash: Online and Offline Cash (cont'd.)

- Main deterrent to double-spending
 - Threat of detection and prosecution
- System must provide tamperproof electronic cash traceable back to origins
 - Two-part lock
 - Provides anonymous security
 - Signals an attempt to double-spend cash that is traceable
- Electronic cash used correctly:
 - Preserves user's anonymity

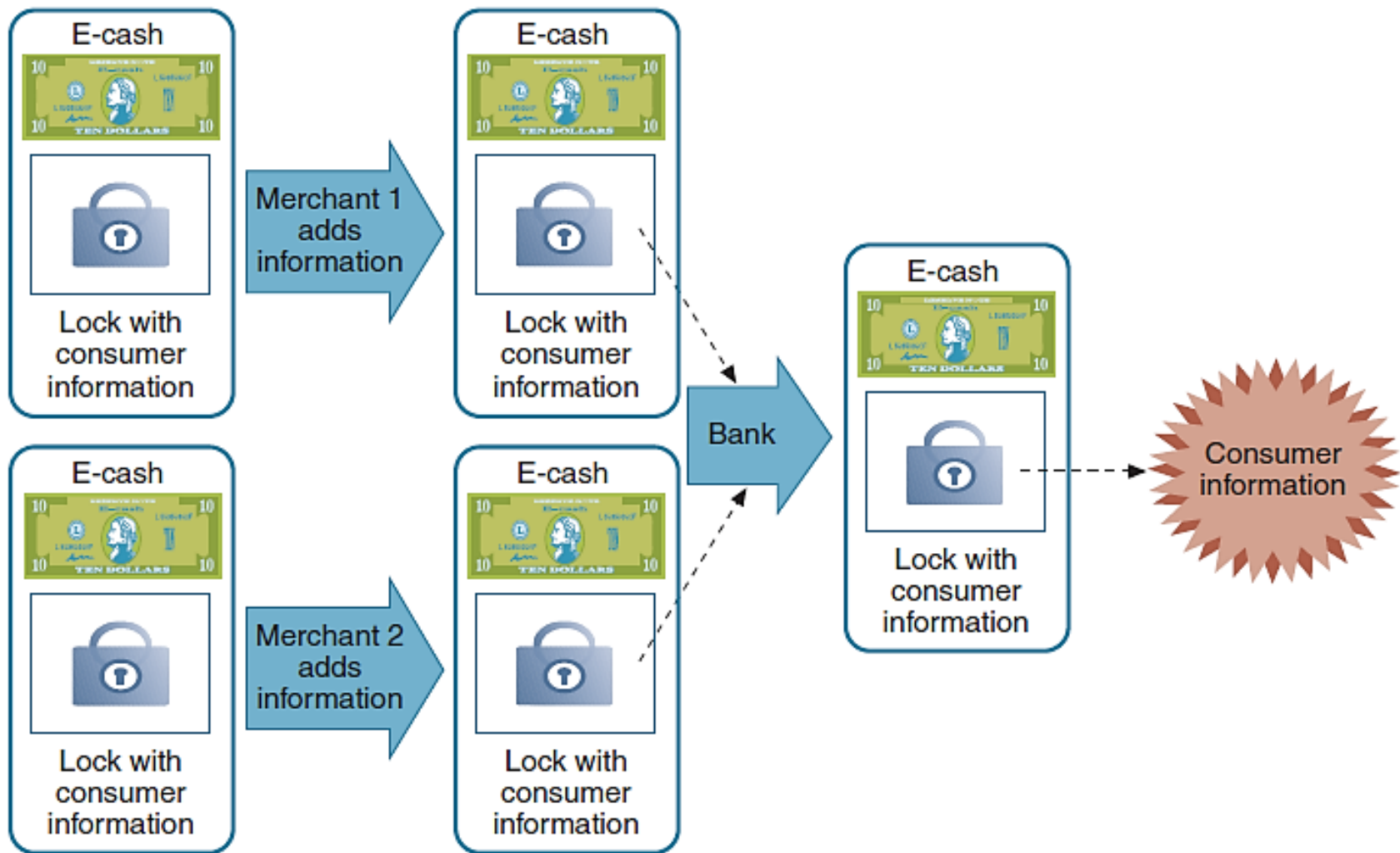


FIGURE 11-4 Detecting double spending of electronic cash

Advantages and Disadvantages of Electronic Cash

- Traditional brick-and-mortar billing methods
 - Costly and inefficient
- Online stores have the same payment collection inefficiencies
- Most online customers use credit cards to pay for purchases

Advantages and Disadvantages of Electronic Cash (cont'd.)

- Electronic cash system
 - Less popular than other payment methods
 - Provides unique advantages and disadvantages
- Advantages of electronic cash transactions
 - More efficient (less costly)
 - Efficiency fosters more business (lower prices)
 - Occurs on existing infrastructure (Internet)
 - Does not require one party to obtain authorization:
 - As required with credit card transactions

Advantages and Disadvantages of Electronic Cash (cont'd.)

- Disadvantages of electronic cash transactions
 - No audit trail
 - **Money laundering**
 - Technique criminals use to convert money illegally obtained into spendable cash
 - Purchase goods, services with ill-gotten electronic cash
 - Goods sold for physical cash on open market

Advantages and Disadvantages of Electronic Cash (cont'd.)

- Electronic cash
 - More successful in Europe and Asia
 - Consumers prefer to use cash (does not work well for online transactions)
 - Electronic cash fills important need
 - Not successful in United States
 - Consumers have credit cards, debit cards, charge cards, checking accounts
- KDD Communications (KCOM)
 - Internet subsidiary: Japan's largest phone company
 - Offers electronic cash through NetCoin Center

Advantages and Disadvantages of Electronic Cash (cont'd.)

- Reasons for failure of United States electronic cash systems
 - Electronic cash systems implementation
 - Requires software installed into consumers' Web browsers
 - Number of competing technologies
 - No standards developed
 - Array of proprietary electronic cash alternatives that are not interoperable
- **Interoperable software:**
 - Runs transparently on variety of hardware configurations and different software systems

Digital Wallets

- Consumer concerns when shopping online
 - Entering detailed shipping and payment information for each online purchase
 - Filling out forms
- Solution
 - Allows customer to store name, address, credit card information on the site
 - Problem
 - Consumers must enter information at each site

Digital Wallets (cont'd.)

- **Digital wallet (electronic wallet or e-wallet)**
 - Holds credit card numbers, electronic cash, owner identification, owner contact information
 - Provides information at electronic commerce site checkout counter
 - Benefit: consumer enters information once
 - More efficient shopping
 - Digital wallet technology elements
 - System: infrastructure for identification
 - Application: software for user interaction
 - Device: applicable if a specific device is used

Software-Only Digital Wallets

- **Server-side digital wallet**
 - Stores customer's information on remote server of merchant or wallet publisher
 - No download time or installation on user's computer
 - Main weakness
 - Security breach can reveal thousands of users' personal information to unauthorized parties

Software-Only Digital Wallets (cont'd.)

- **Client-side digital wallet**
 - Stores information on consumer's computer
 - Disadvantages
 - Not portable: must download wallet software onto every computer
 - Advantage
 - Sensitive information stored on user's computer

Software-Only Digital Wallets (cont'd.)

- Server-side digital wallet examples:
 - Microsoft Windows Live ID
 - Single sign-in (SSI) service
 - Completes order forms automatically
 - Personal data encrypted and password protected
 - Integrated services: SSI, Wallet service, Kids service, public profiles
 - Yahoo! Wallet
 - Software-based digital wallet
 - Automatically fills online forms
 - Accepted by large number of merchants

Hardware-Based Digital Wallets

- Implemented using smart phones
 - Store owner's identity credentials (driver's license, medical insurance card, store loyalty cards, etc.)
 - Transmit portions of identify information using:
 - Bluetooth or wireless transmission to nearby terminal
 - **Near field communication (NFC)** technology: contactless wireless transmission of data over short distances

Hardware-Based Digital Wallets (cont'd)

- Status:
 - Popular in Japan: mobile phones with NFC chips
 - *Oisaifu-Keitai* (“mobile wallet”)
 - U.S. examples:
 - Google Wallet (uses PayPass technology)
 - V.me (Visa digital wallet)
 - PayPal digital wallet (release anticipated)

Stored-Value Cards

- Microchip smart card or magnetic strip plastic card
- Examples: credit cards, debit cards, charge cards, driver's license, health insurance card, and employee or student identification card

Magnetic Strip Cards

- Holds rechargeable value
- Passive magnetic strip cards cannot:
 - Send or receive information
 - Increment or decrement cash value stored
- Processing done on device into which card inserted

Smart Cards

- **Smart card (stored-value card):**
 - Plastic card with embedded microchip
- Credit, debit, charge cards store limited information on magnetic strip
- Information storage
 - About 100 times more than magnetic strip plastic card
- Holds private user data
 - Financial facts, encryption keys, account information, credit card numbers, health insurance information, medical records

Smart Cards (cont'd.)

- Safer than conventional credit cards
 - Information encrypted on smart card
- Popular in Europe, parts of Asia
 - Public telephone calls, cable television programs
 - Hong Kong
 - Retail counters, restaurant cash registers have smart card readers
 - Octopus: public transportation smart card can be reloaded at transportation locations, 7-Eleven stores

Smart Cards (cont'd.)

- Beginning to appear in United States
 - San Francisco TransLink integrated ticketing system for public transportation
- **Smart Card Alliance**
 - Advances smart card benefits
 - Promotes widespread acceptance of multiple-application smart card technology
 - Promotes compatibility among smart cards, card reader devices, applications

Internet Technologies and the Banking Industry

- Paper checks
 - Largest dollar volume of payments
 - Processed through world's banking system
- Other major payment forms
 - Involve banks one way or another
- Banking industry Internet technologies
 - Providing new tools
 - Creating new threats

Check Processing

- Old method of physical check processing
 - Person wrote check; retailer deposited check in bank account
 - Retailer's bank sent paper check to clearinghouse
 - Clearinghouse managed fund transfer (consumer's bank to retailer's account)
 - Paper check transported to consumer's bank
 - Cancelled check sent to consumer
- Banks now provide PDF images of processed checks

Check Processing (cont'd.)

- Disadvantage of paper checks
 - Cost of transporting tons of paper checks
 - Float
 - Delay between the time person writes check and the time check clears person's bank
 - Bank's customer obtains free use of funds for few days
 - Bank loses use of funds for same time period
 - Can become significantly longer than a few days

Check Processing (cont'd.)

- Technologies helping banks reduce float
 - 2004 U.S. law: Check Clearing for the 21st Century Act (**Check 21**)
 - Banks eliminate movement of physical checks entirely
- Check 21-compliant world
 - Retailer scans customer's check
 - Scanned image transmitted instantly
 - Through clearing system
 - Posts almost immediately to both accounts
 - Eliminates transaction float

Mobile Banking

- Banks exploring mobile commerce potential
- 2009: banks launched sites allowing customers using smart phones to:
 - Obtain bank balance, view account statement, and find a nearby ATM
- Future plans
 - Offering smart phone apps
 - Use to transact all types of banking business
- Credit card reader attachment available for some smart phones yielding a portable payment processing terminal

Criminal Activity and Payment Systems: Phishing and Identity Theft

- Online payment systems
 - Offer criminals and criminal enterprises an attractive arena in which to operate
 - Average consumers: easy prey
 - Large amounts of money provide tempting targets
 - Phishing expedition
 - Technique for committing fraud against online businesses customers
 - Particular concern to financial institutions

Phishing Attacks

- Basic structure
 - Attacker sends e-mail message:
 - To accounts with potential for an account at targeted Web site
 - E-mail message tells recipient: account compromised
 - Recipient must log on to account to correct problem
 - E-mail message includes link
 - Appears to be Web site login page
 - Actually leads to perpetrator's Web site disguised to look like the targeted Web site

Phishing Attacks (cont'd.)

- Recipient enters login name, password
 - Perpetrator captures
 - Uses to access recipient's account
 - Perpetrator accesses personal information, makes purchases, withdraws funds

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

FIGURE 11-5 Phishing e-mail message

E-Business, Tenth Edition

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](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 11-5 Phishing e-mail message (cont'd.)

Phishing Attacks (cont'd.)

- **Spear phishing**
 - Carefully designed phishing expedition targeting a particular person or organization
 - Requires considerable research
 - Increases chance of e-mail being opened
 - Example: 2008 government stimulus checks
 - Phishing e-mails appeared within one week of passage

Phishing Attacks (cont'd.)

- E-mail link disguises and tricks
 - Example: Web server ignores all characters preceding “@”:
 - <https://www.paypal.com@218.36.41.188/fl/login.html>
 - Link appears different in e-mail
 - Phony site invisible due to JavaScript code
 - Pop-up windows
 - Look exactly like browser address bar
 - Including Web site graphics of financial institutions
 - Looks more convincing

Phishing Attacks (cont'd.)

- Web sites to learn more about phishing techniques:
 - Conferences on Email and Anti-Spam
 - Anti-Phishing Working Group (APWG)

From: Bank of America <BankofAmerica@service.com>
Subject: Bank of America Notices : Your Online Account Security Status
To: [Emailaddress removed]
Date: [Date removed]



Online Banking Alert

Verification of your current details.

Remember:
You are expected to complete this update not later than 2 working days from the receipt of this mail.

Dear Valued Customer :

During our regular update and verification of the Bank of America Online Banking Service, we could not verify your current information. Either your information has been changed or incomplete, as a result your access to use our services has been limited. Please update your information.

To restore your online banking access, kindly update your information. You can update your online banking details by following the link below.

[Click here to update your account!](#)

Thank you for banking with Bank of America, the industry leader in safe and secure online banking

Sincerely,
Bank of America Customer Service

FIGURE 11-6 Phishing e-mail with graphics


Our paperless statements securely store your statements online for you to view up to 18 months of activity. [Learn more](#).

Important

Because E-Mail Is Not A Secure Form Of Communication, This E-Mail Box Is Not Equipped To Handle Replies.

If you are a Bank of America customer and have sensitive account-related questions, please call the phone number provided on your account statement or the appropriate phone number indicated in the following "Contact Us" link so we can properly verify your identity. For all other questions or comments, please use the Web forms available via [Contact Us](#). We respect your privacy, and you can rest assured that we protect your information, including your email address, and will never sell or share it with marketers outside Bank of America.

To find out more, please read our [Privacy Policy](#). Bank of America E-mail, 6th Floor, 101 North Tryon Street, Charlotte, NC 28255-0001

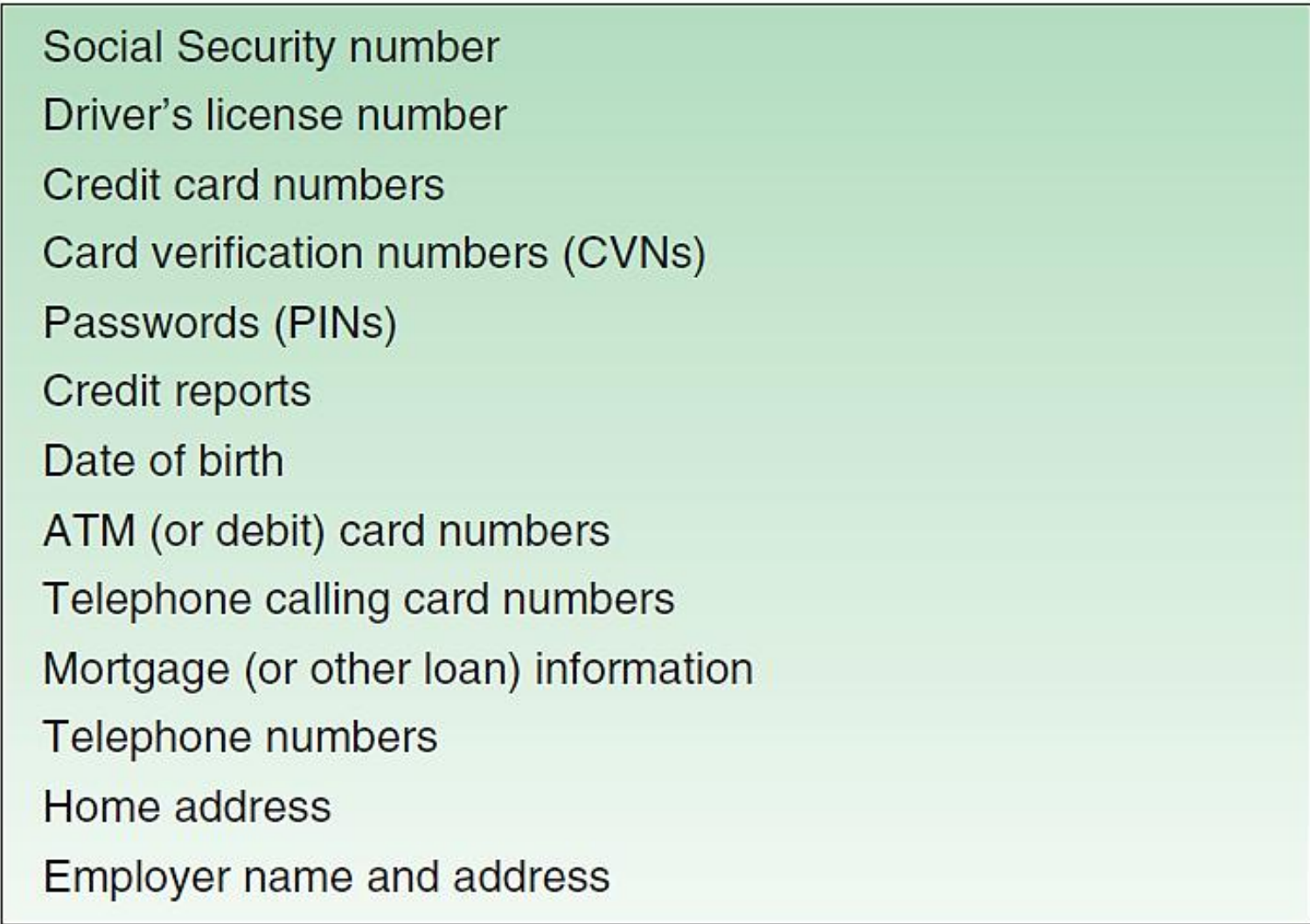
Bank of America, N.A. Member FDIC. [Equal Housing Lender](#) 
© 2006 Bank of America Corporation. All Rights Reserved.

Official Sponsor 2004-2008
U.S. Olympic Teams 

FIGURE 11-6 Phishing e-mail with graphics (cont'd.)

Using Phishing Attacks for Identity Theft

- **Organized crime (racketeering)**
 - Unlawful activities conducted by highly organized, disciplined association for profit
 - Differentiated from less-organized groups
 - Internet providing new criminal activity opportunities
 - Generates spam, phishing, identity theft
- **Identity theft**
 - Criminal act: perpetrator gathers victim's personal information
 - Uses information to obtain credit
 - Perpetrator runs up account charges and disappears



- Social Security number
- Driver's license number
- Credit card numbers
- Card verification numbers (CVNs)
- 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 name and address

FIGURE 11-7 Types of personal information most useful to identity thieves

Using Phishing Attacks for Identity Theft (cont'd.)

- Large criminal organizations
 - Efficient perpetrators of identity theft
 - Exploit large amounts of personal information quickly and efficiently
 - Sell or trade information that is not of immediate use
 - Other worldwide organized crime entities
 - **Zombie farm**
 - Large number of computers implanted with zombie programs
 - **Pharming attack**
 - Use of a zombie farm, often by an organized crime association, to launch a massive phishing attack

Using Phishing Attacks for Identity Theft (cont'd.)

- Two elements in phishing
 - **Collectors:** collect information
 - **Cashers:** use information
 - Require different skills
- Crime organizations facilitate transactions between collectors and cashers
 - Increases phishing activity efficiency and volume
- Each year:
 - More than a million people fall victim
 - Financial losses exceed \$500 million

Phishing Attack Countermeasures

- Change protocol
 - Improve e-mail recipients' ability to identify message source
 - Reduce phishing attack threat
- Educate Web site users
- Contract with consulting firms specializing in anti-phishing work
- Monitor online chat rooms used by criminals

Summary

- Online stores: payment forms
 - Credit, debit, charge cards (payment cards)
 - Ubiquitous, convenient, and easy to use
 - Electronic cash: portable and anonymous online payment form
 - Useful for micropayments
 - Digital wallets provide convenience
 - Stored-value cards
 - Smart cards, magnetic strip cards

Summary (cont'd.)

- Banks process most monetary transactions
 - Use Internet technologies to process checks
- Concerns: phishing expeditions, identity theft