



# CHAPTER ELEVEN

## Payment System for E-Commerce

# Introduction

- **Financial technology (fintech)** is the use of powerful Internet-connected computers that use tools such as Web services to improve quality and reduce cost of services
  - More importantly, to create entirely new types of financial products and services
    - Including payment services not operated by banks at all
      - Facilitates purchases and other money transfers
      - Convenient and becoming widely adopted
    - Has also revolutionized lending
      - Online loan services takes banks out of value chain at a reduced cost

# Common Online Payment Methods

- Cash, checks, credit cards, debit cards are the four most common methods used in the world to **pay for purchases**
  - Account for more than 90% of all US consumer payments today
- The use of credit and debit cards will continue to **decrease**
- An increasing proportion of all of these payments are made using **mobile devices**

# Electronic Bill Presentment and Payment Systems (EBPP)

- Designed to **deliver bills and accept payments** for customers
  - Success depends on ease of use and time required
- Consumers choosing this option is **increasing**
  - 70% of bills paid by check are now paid electronically which is a huge savings in paper, postage and time
- **Biller-direct systems** are used by large companies who want to manage and maintain the systems themselves
- **Consolidator systems** aggregate all a customer's bills on one system mostly via banks
  - Not **as attractive to** billers because the consolidator providing the service must be paid a fee and a delay is introduced into the system.

# Micropayments and Small Payments

- **Micropayments** are Internet payments for items costing from a few cents to approximately a dollar
  - **Barrier** is people prefer to buy small value items in fixed price chunks rather than small payments in varying amounts
  - Many companies have developed micropayment systems but **none** gained broad acceptance
- **Small payments** are payments of less than \$10
  - Offered through mobile telephone carrier but held back by substantial charges for providing service
    - One of the largest markets is music downloads

# Payment Cards

- **Payment cards** are all types of **plastic cards** used for purchases
  - **Categories:** credit cards, debit cards, charge cards, prepaid cards, and gift cards
- **Credit cards** (Visa, MasterCard) have a **spending limit** based on user's credit history
  - A user can pay off entire credit card balance or minimum amount with interest charged on unpaid balances
  - Widely accepted and provides consumer protection: 30-day dispute period
  - Online and telephone purchases are often called **card not present transactions**
  - *Card not present transactions* include an extra degree of risk for merchant and bank

# Payment Cards (cont'd.)

- **Debit card** (electronic funds transfer at point of sale (EFTPOS) cards) removes funds from cardholder's bank account and transfers it to seller's account
  - Issued by bank with major credit card issuer's name
- **Charge card** (American Express) has no spending limit with entire amount due at end of billing period
  - Retailers may offer their own store charge cards
- **Prepaid cards** are called gift cards
- **Single-use cards** had disposable numbers, valid for one transaction, but not attracted to consumers

# Advantages and Disadvantages of Payment Cards

- **Advantage for merchants** include fraud protection
  - Can authenticate and authorize purchases using a payment card processing network
  - Interchange network is a set of connections between banks that issue credit cards, the associations that own the credit cards (such as MasterCard or Visa), and merchants' banks.
- **Advantage for U.S. consumers** is limited fraud liability of \$50 which is often waived if card is stolen
- Merchants view the per-transaction and monthly processing fees as a cost of doing business
- Consumers pay a slightly higher cost for goods due to these cards and some charge an annual fee

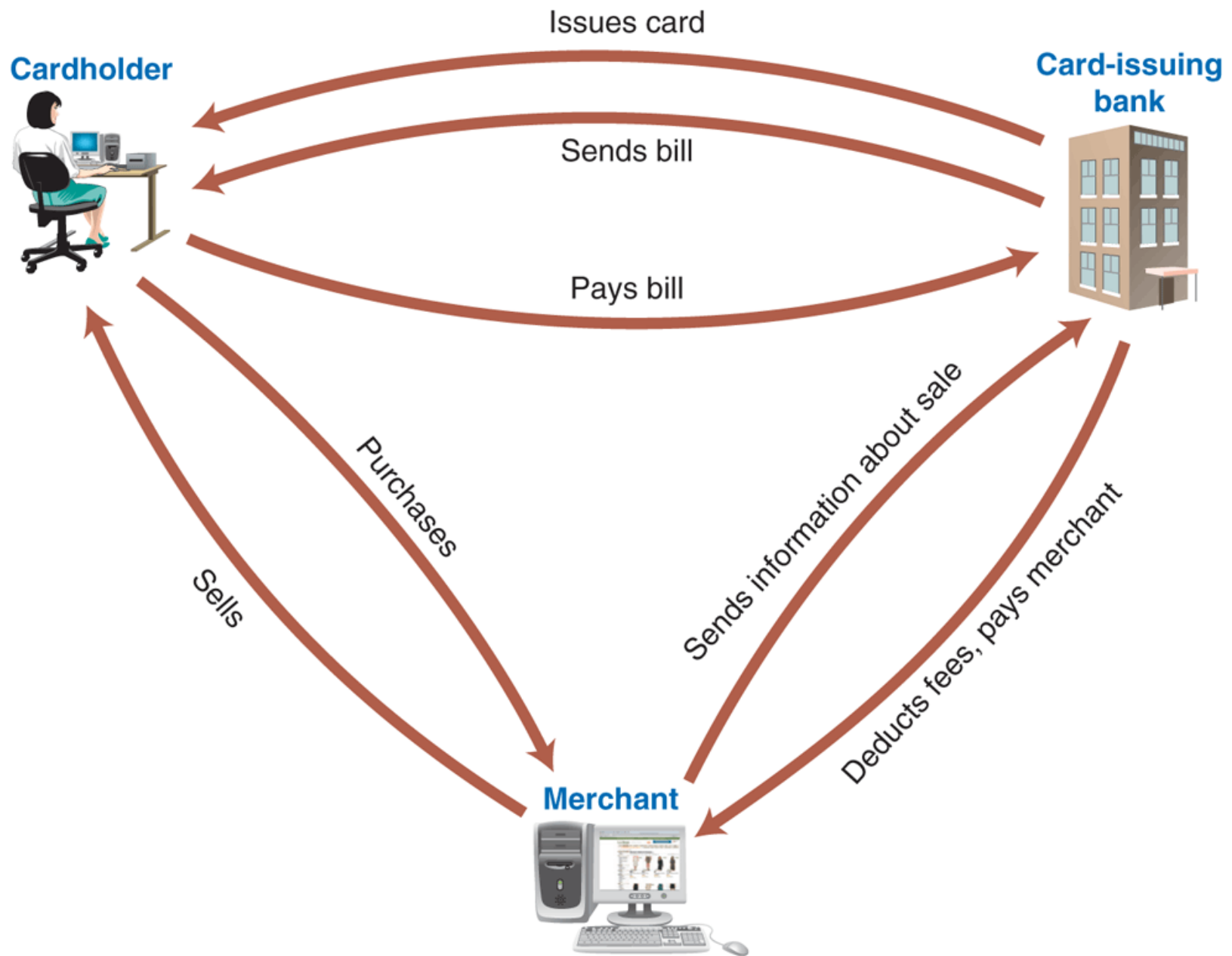


# Payment Acceptance and Processing

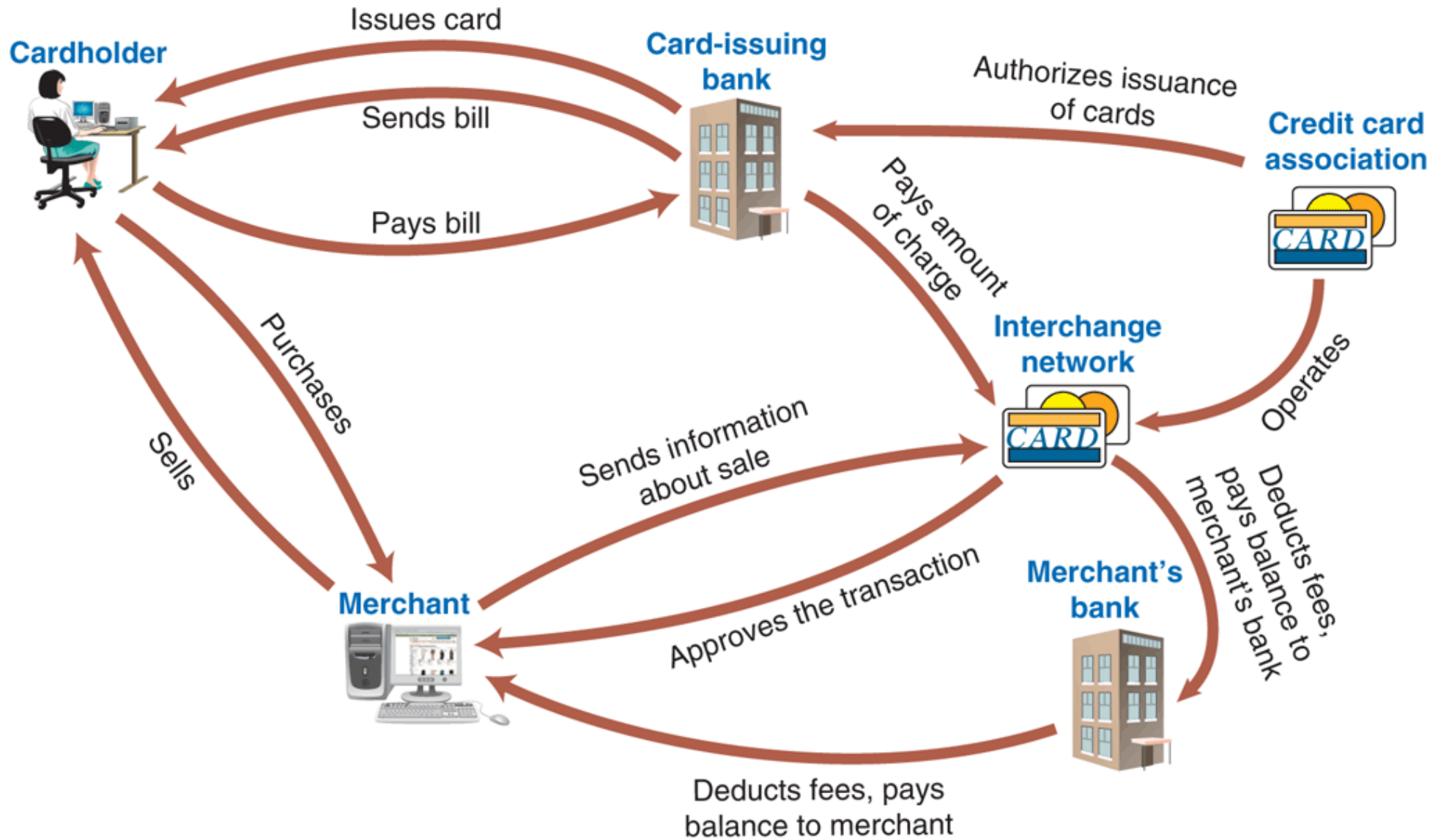
- US online and mail order stores must **ship merchandise** within **30 days** of charging payment
  - Significant violation penalties
  - So most stores do not charge payment card accounts until they ship merchandise
- Processing payment card transactions online is a **two step** process
  - **Payment acceptance** is establishing card validity and verifying card's limit not exceeded by transaction
  - **Clearing the transaction** includes all steps to move funds from card holder's bank account into the merchant's bank account

# Open and Closed Loop Systems

- With **a closed loop system** the card issuer pays merchant directly without a bank or clearinghouse
  - American Express, Discover Card
  - Issue cards directly to consumers
- **Open loop systems** add additional payment processing intermediaries to the closed loop system
  - Visa, MasterCard issued by local bank
  - Visa and MasterCard are **credit card associations** operated by customer issuing banks who evaluate credit standing, establish credit limits and absorb non-payment losses



**FIGURE 11-2 Closed loop payment card system**



**FIGURE 11-3 Open loop payment card system**

# Online Antifraud

- Level of fraud is **higher** online
  - Under 15% of all credit card transactions responsible for 64% percent of total dollar amount of credit card fraud (declining since 2008)
- Antifraud measures include
  - Scoring services that provide risk ratings for individual transactions in real time
  - Shipping only to card billing address and requiring **card verification numbers (CVNs)** for card not present transactions
    - Three- or four-digit number printed on the credit card but not encoded on the card's magnetic strip

# Stored-Value Cards

- **A stored-value card** is a plastic card with embedded microchip that can store information and perform calculations
  - Most incorporate **near field communication (NFC)** technology which allows for contactless data transmissions over short distances
    - Allows interacts with readers and other devices
- Can hold much more data than a magnetic card
  - Safer because data can be encrypted
- Used in Europe and Asia but less successful in U.S.
  - U.S. use has increased in recent years but still not widespread

# Digital Cash

- Also called **electronic cash or e-cash**
- Is a general term that 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
  - No common standard adopted so far
- Can be held in online storage or offline storage

# Digital Cash (cont'd.)

- With **online** cash storage consumer has no personal possession of digital cash
  - Trusted third party (online bank) involved in all transfers, holds consumers' cash accounts
  - Merchant contacts consumer's bank for payment
  - Helps prevent fraud (confirm valid cash)
- Fills a need in developing countries that rely on cash as they conduct B2C electronic commerce
  - Need does not exist here because U.S. consumers already have payment cards

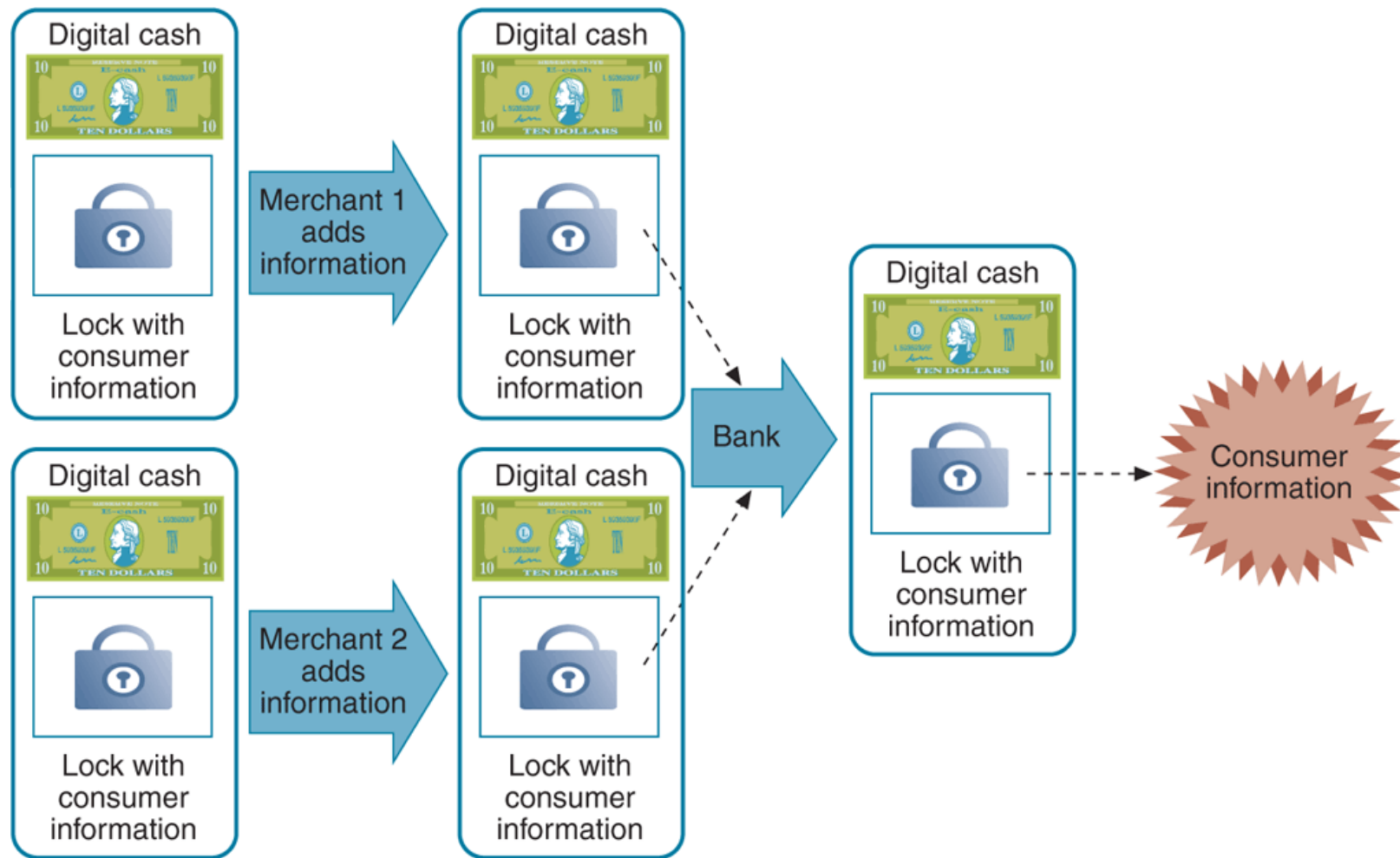


# Digital Cash (cont'd.)

- **Bitcoin** is the most well-known provider today
  - Online ledger book that tracks balances while participants remain anonymous
  - Public-key cryptography is used (the first popular cryptocurrency)
  - Large percentage of uses involve illegal purchases and currency speculation (because of its anonymity)
- **Concerns** include privacy and security, independence, portability, convenience
  - Must be impossible to spend more than once, easy to use and not traceable to the person who spent it
    - Anonymous digital cash

# The Double-Spending Issue

- Spending a particular piece of digital cash **twice** by submitting the **same** electronic currency to **two** different vendors
  - When the electronic currency reaches the bank for clearance a second time, it is **too late** to prevent the fraudulent act
  - Main deterrent is threat of **detection and prosecution** so system must provide traceability back to origin
- Two-part lock provides anonymous security and signals when someone is attempting to double spend cash



**FIGURE 11-4** Detecting double spending of electronic cash

# Advantages and Disadvantages of Digital Cash

- Can be more efficient (less costly) than traditional payment methods
  - Less than processing credit card transactions or conventional money exchange systems
  - Does not require authorization
- **No audit trail** (similar to physical cash) makes it non-traceable which can lead to money laundering
  - **Money laundering** is a technique to convert illegally-obtained money into money spendable without being linked to illegal activity

# Digital Wallets and Software-Based Digital Wallets

- A **digital wallet** is an electronic device or software that can store credit card numbers, digital cash, owner identification, and owner contact information and provide that information to an online business at checkout
  - Benefit is customer enters information just once
- **Server-side digital wallet** stores information on remote server belonging to a particular merchant or wallet publisher
  - Security breach can reveal thousands of users' personal information to unauthorized parties
  - Widely used examples: Google Wallet, Microsoft Windows Live ID, Yahoo! Wallet
- **Client-side digital wallet** stores information on consumers computers
  - Must download wallet software onto every computer

# Hardware-Based Digital Wallets

- Implemented using **smart phones or tablets**
- Store owner's identity credentials (driver's license, medical insurance card, store loyalty cards, etc.)
- Transmit portions of information using Bluetooth or wireless transmission to nearby terminal
- Near field communication (NFC) technology can be used if equipped with NFC chip
- Examples: Google Wallet, Android Pay and Apple Pay
- Security and privacy are major concerns
  - Must prevent unauthorized access

# Internet Technologies and the Banking Industry



- Paper checks still the largest dollar volume of payments in the world today
  - Processed through world's banking system
- Other major payment forms also involve banks
- Internet technologies are providing new tools and creating new threats for the banking industry

# Check Processing

- Old method of physical check processing
  - Person wrote check which was deposited by retailer and sent to clearinghouse to manage funds transfer
  - Paper check transported to consumer's bank and cancelled check sent to consumer
  - Disadvantages include **transportation cost** and **float**
    - Float: delay between time check is written and clears
- Check Clearing for the 21st Century Act (Check 21) permits bank to eliminate movement of physical checks and use image scanning technology
  - Instant check clearing eliminates float



# Payment System Threats: Phishing and Identity Theft

- Online payment systems offer attractive arena for criminals and criminal enterprises
- **Phishing attacks** are techniques for committing fraud against online businesses customers
  - Particular concern to financial institutions

# Phishing Attacks

- Attacker sends e-mail message to accounts with potential for an account at targeted Web site
  - E-mail message tells recipient account compromised and recipient must log in to correct problem
    - Includes link that appears to be Web site login page
    - Actually leads to perpetrator's site so that victim's log in information can be captured and used
- **Spear phishing** is a carefully designed phishing attack targeting a particular person or organization
  - Requires considerable research which increases chance of e-mail being opened

**FIGURE 11-5**  
Phishing e-mail  
message

Date: xx-xx-xx-xx  
From: xx-xx-xx-xx  
Subject: xx-xx-xx-xx  
To: xx-xx-xx-xx

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: xx-xx-xx-xx

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:  
[xx-xx-xx-xx](#)

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 xxxxx

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

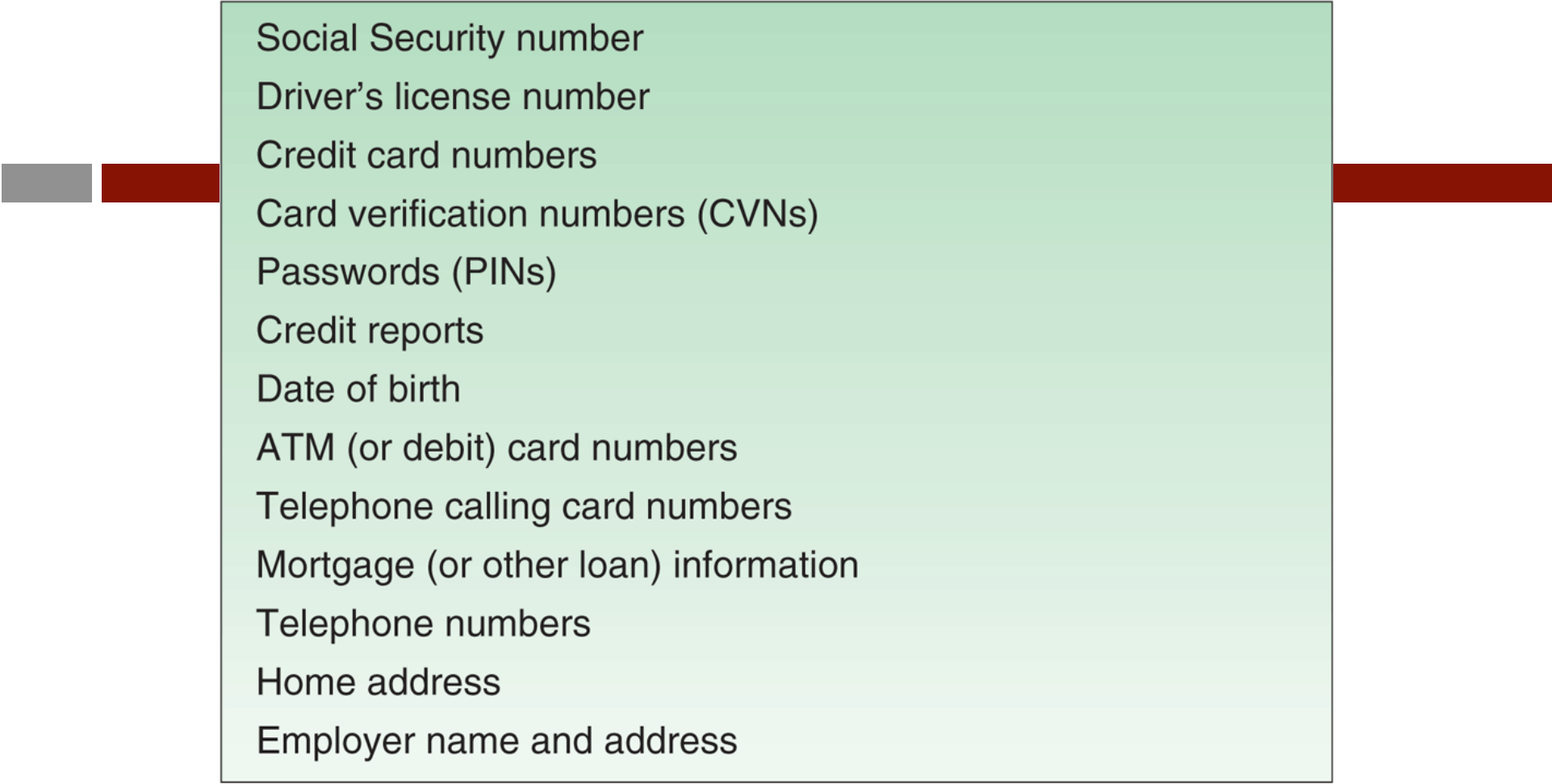
Visit our Privacy Policy and User Agreement if you have any questions.  
[xx-xx-xx-xx](#)

# Phishing Attacks (cont'd.)

- Example: 2008 government stimulus checks
  - Phishing e-mails that seemed to be from the IRS appeared within one week of passage
- E-mail link disguise the real URL by using “@” which causes the Web site to ignore characters before it
  - <https://www.paypal.com@218.36.41.188/fl/login.html>
  - Phony site invisible due to JavaScript code
- Pop-up windows look exactly like browser address bar including Web site graphics to make it even more convincing

# Using Phishing Attacks for Identity Theft

- Organized crime (racketeering) is 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 is a criminal act where perpetrator gathers victim's personal information
  - Goal is 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 11-6** Types of personal information most useful to identity thieves

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

- Large criminal organizations can be highly efficient perpetrators of identity theft
- **Zombie farm** is a large number of computers implanted with zombie programs
  - **Pharming attack** is the use of a zombie farm, often by organized crime, to launch a massive phishing attack
- Phishing needs both collectors and cashers (users) of information which requires different skills
  - Crime organizations increase efficiency and volume by facilitating and participating in these transactions
  - Over a million victims and \$1.5 billion lost annually

# Phishing Attack Countermeasures

- Spam is a key element of phishing attacks
  - Any protocol changes that improve e-mail recipients' ability to identify message source reduces phishing
- Educate Web site users
- Contract with consulting firms specializing in anti-phishing work
  - Monitor online chat rooms used by criminals
- Incidence of phishing has grown rapidly over the past two years and experts expect it will continue
  - Extremely profitable criminal activity