Cool Tech Club
E-commerce Fraud and Fraud Mitigation

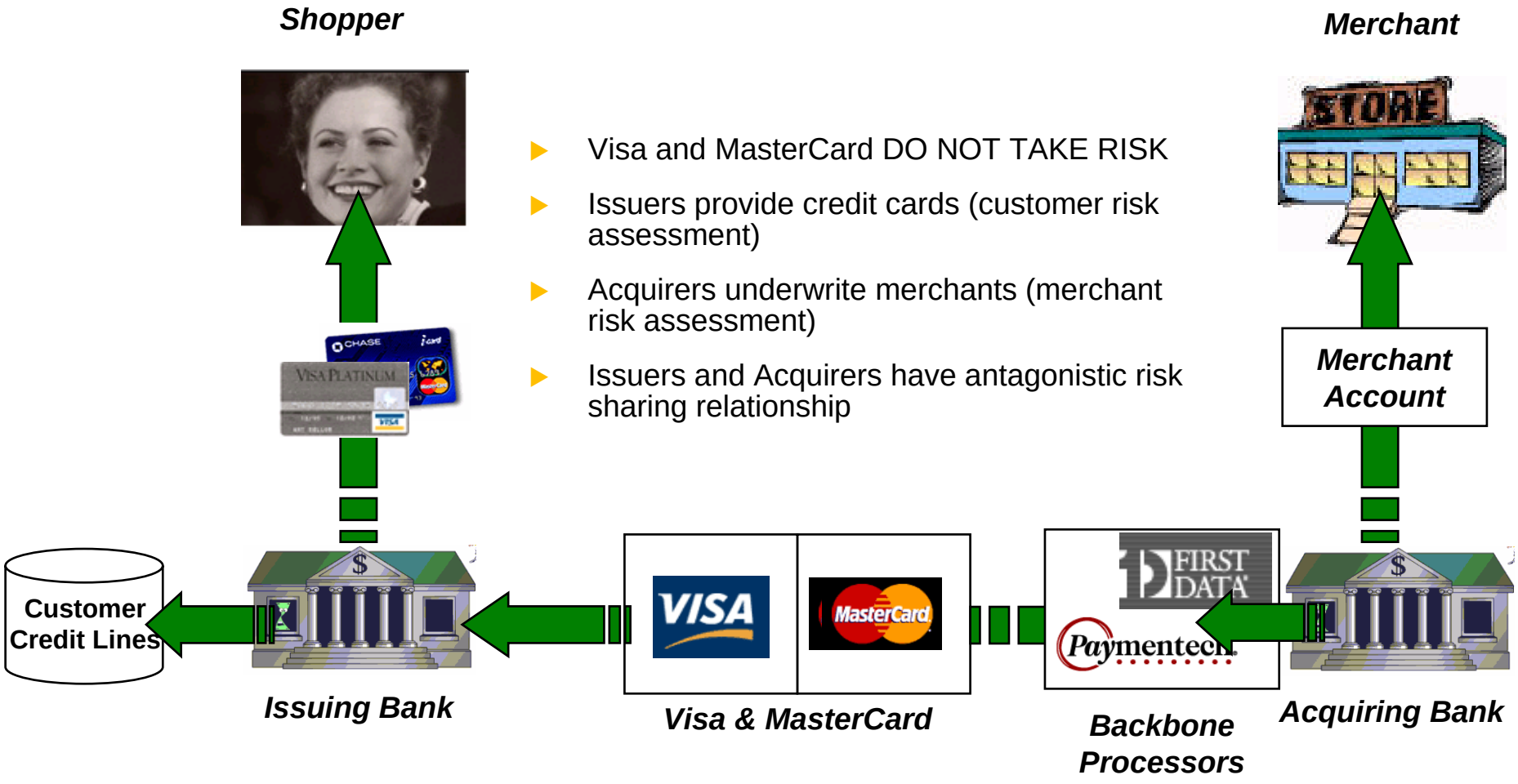
Steve Manning
August 25, 2004

Overview

- Fundamentals of online transactions
- Trends in online fraud
- How fraud happens
- Protection Against Fraud

Fundamentals of Online Transactions

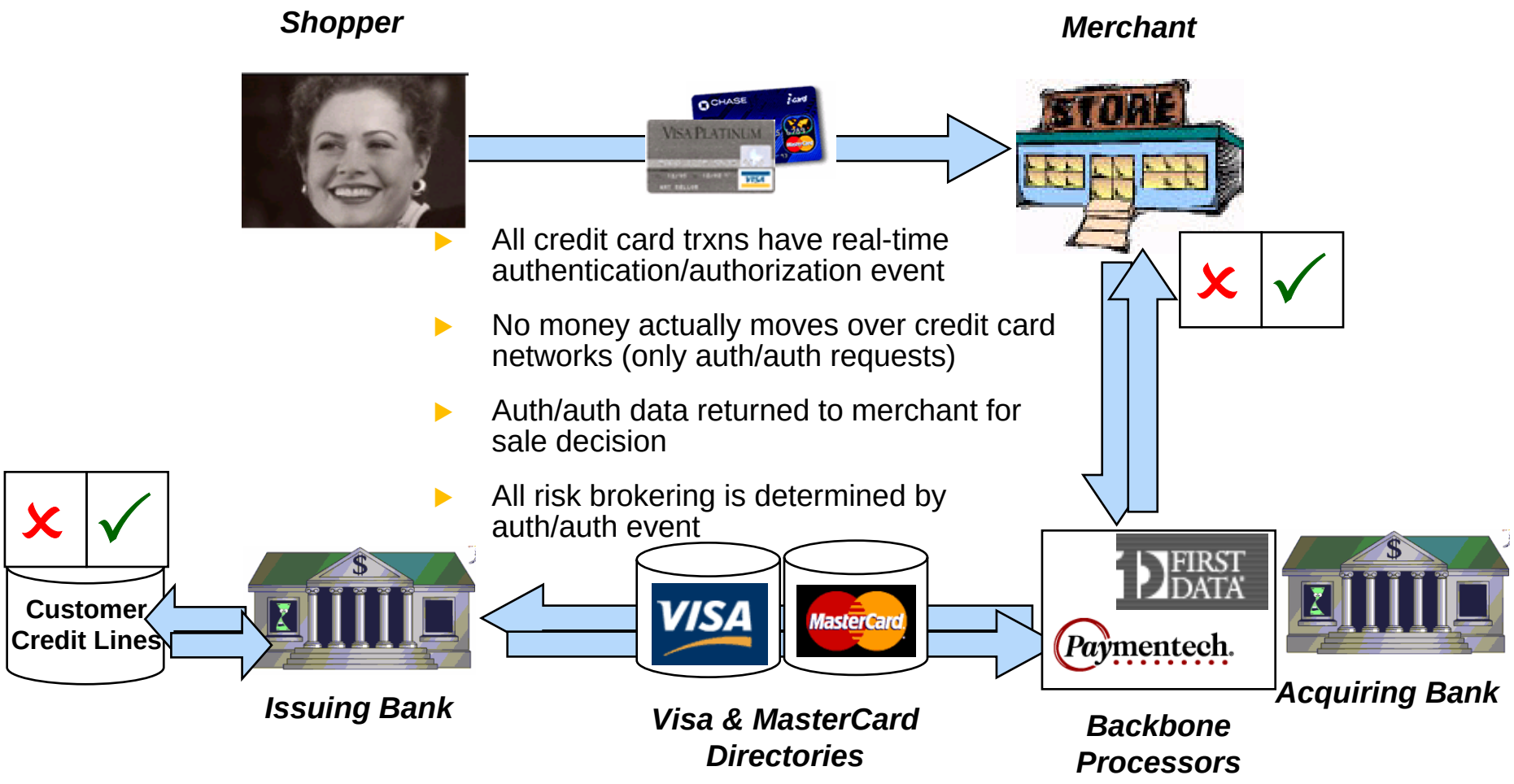
How it works: Set-up



- Visa and MasterCard DO NOT TAKE RISK
- Issuers provide credit cards (customer risk assessment)
- Acquirers underwrite merchants (merchant risk assessment)
- Issuers and Acquirers have antagonistic risk sharing relationship

Fundamentals of Online Transactions

How it works: Real-time Authorization



Fundamentals of Online Transactions

How it works: Settlement of Funds

Shopper

End of Billing Cycle: (Check/ACH)

- Consumer does not pay until end of billing cycle
- Fraudulent purchases may not be discovered for 30 days (or more)
- Dispute resolution processes are highly defined by Visa/Mastercard

Merchant

End of Day (ACH)

Customer Credit Lines

Issuing Bank

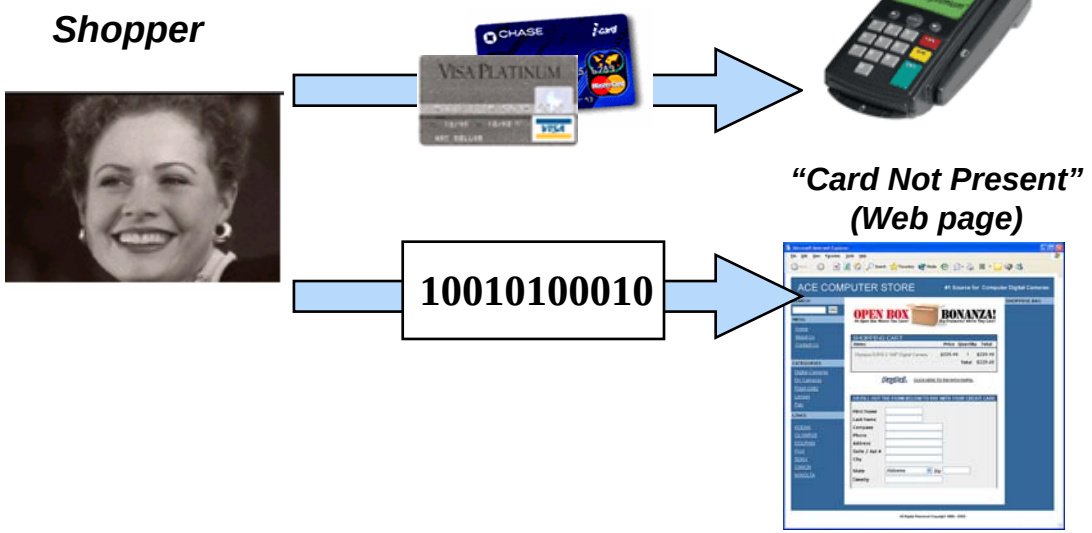
Visa & MasterCard Directories

Backbone Processors

Acquiring Bank

Fundamentals of Online Transactions

Authentication and the input problem



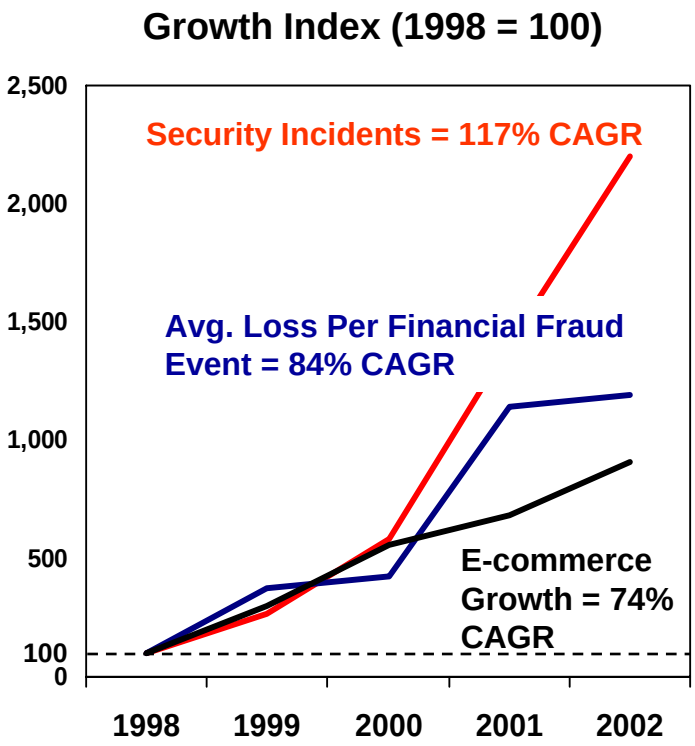
- Limited risk
- Authenticated credential (card)
- Authenticated individual (signature)
- Merchant rarely burned <.1% fraud rate

Merchant

- High risk
- No credential
- No identity authentication
- Merchant frequently burned >1% fraud rate

Trends in Online Fraud

Trend #1: Web crime growing faster than web commerce



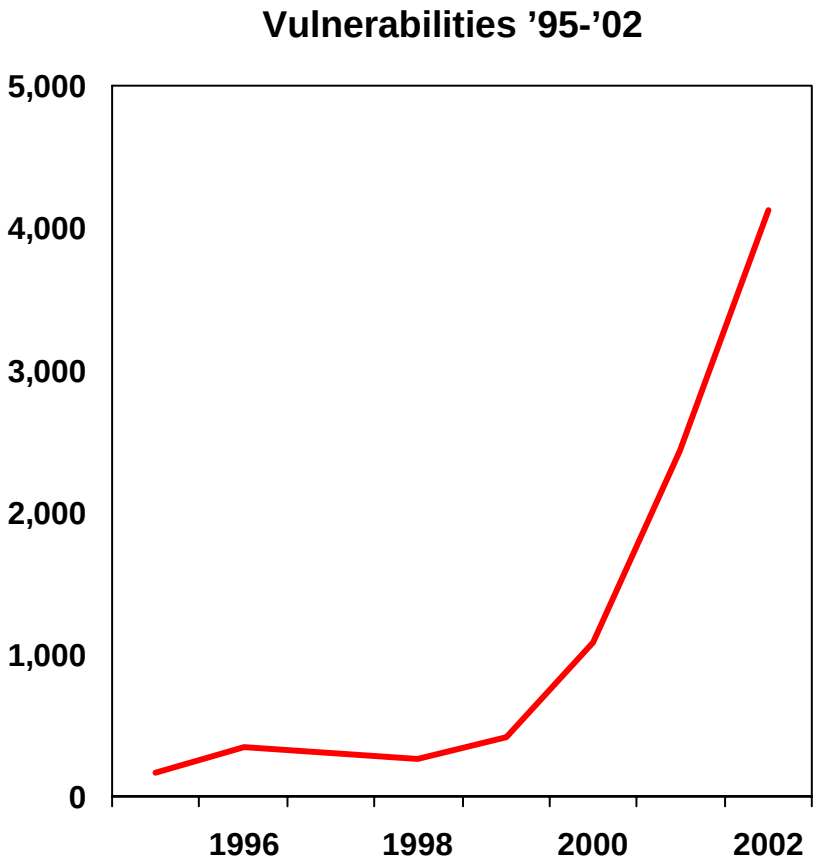
Snapshots From 2002

- *FBI internet fraud center complaints **triple***
- *Online credit card fraud **17 times** offline fraud*
- ***1 in 6** web users had card info stolen*
- ***1 in 12** web users had identity stolen*

Source: FBI/CSI, US Census Bureau, CERT, Gartner 12/02, VeriSign

Trends in Online Fraud

Trend #2: Explosion in known vulnerabilities overwhelms IT resources



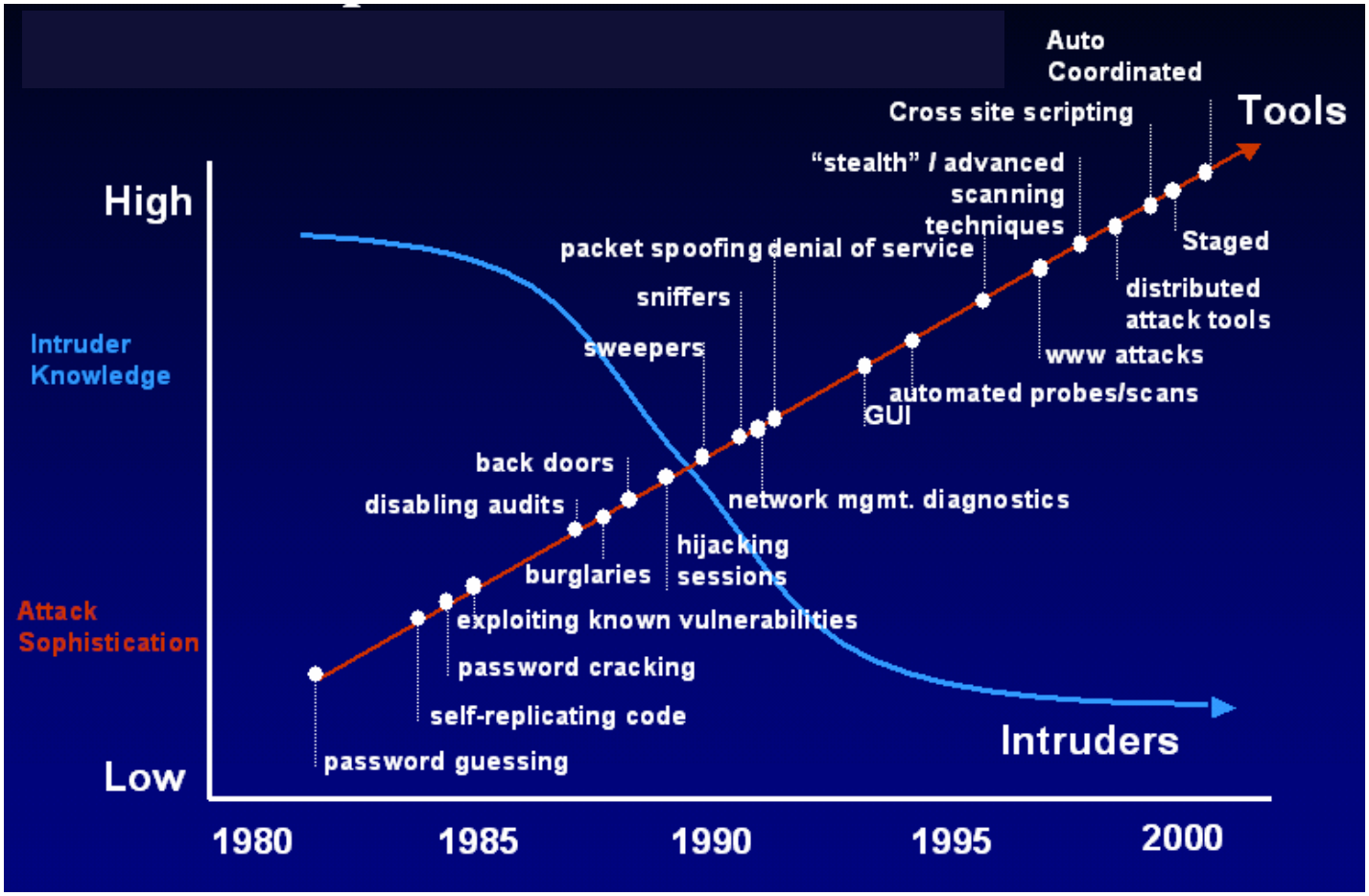
Source: CERT, Symantec, Digex, VeriSign

Snapshots From 2002

- ***99%** of intrusions result from known vulnerabilities or configuration errors*
- *Microsoft released **72 patches** in '02*
- *Redhat released **38 patches** in '02*
- *New vulnerabilities discovered per week: **5 in 1998** to **50 in '02***
- *Published vulnerabilities notify hackers as well as businesses*

Trends in Online Fraud

Growth in vulnerabilities opens infrastructure to myriad of attacks



Source: CERT

Trends in Online Fraud

Trend #3: Automation, collaboration, internationalization

- **Automation**
  - Use of software tools to speed up hacking process
  - Tools lower bar for technical sophistication of hackers

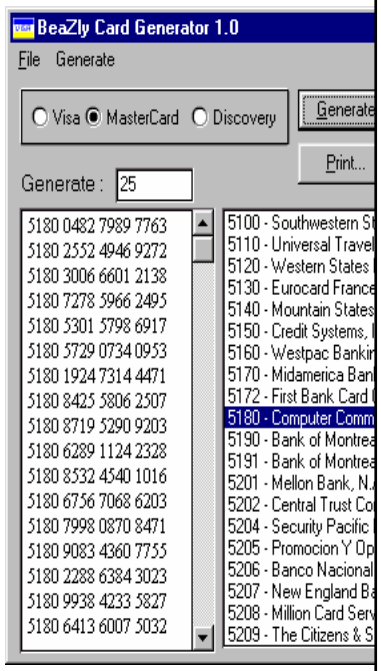
- **Collaboration**
  - Information sharing drives rapid evolution of hacking techniques
  - Specialists easily recruited to hacker teams
  - Businesses do not collaborate as effectively as hackers

- **Internationalization**
  - Over 50% of payments fraud originates from overseas (from a short list of politically instable countries)
  - Current hotspots: eastern europe, asia
  - Internationalization complicates police jurisdiction and prosecution

Trends in Online Fraud

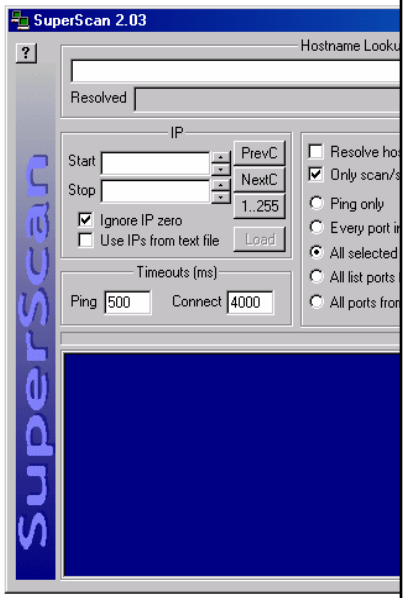
Technology has greatly automated criminal activity

Card Generator



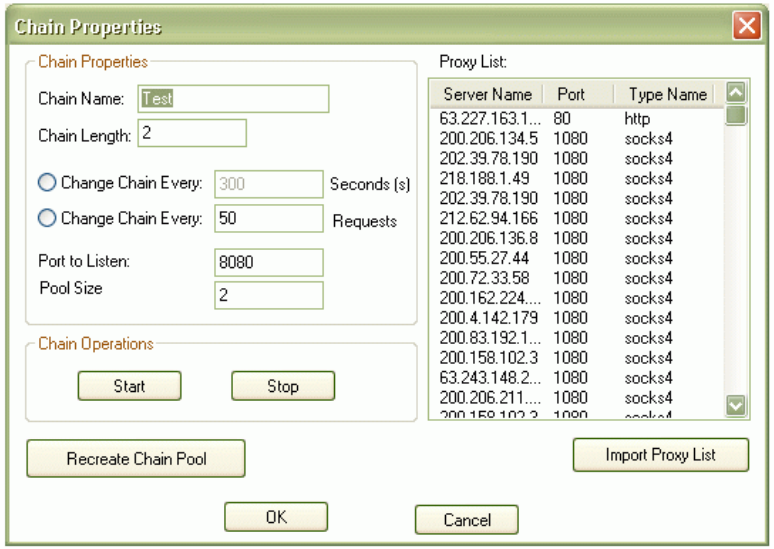
- Software applica
- Mirrors issuer lo
- Spoofs address

Port Scanner



- Software applicati
- Identifies network
- Identifies attack p

Proxy Hopper



- Software application
- Network anonymizer
- Cycles through proxy lists to hide customer origin

Trends in Online Fraud

Collaboration arms hackers with the best information to perpetrate fraud

Card Black Markets

- Identities openly bought and sold
- Ability to spoof many consumer authe
  Soc Sec No.)

Information Sharing Chat Rooms

- Compromised IP lists for anonymizing
- Admin access passwords
- Hack attack methods

Trends in Online Fraud

Trend #4: Government and credit card regulation

- **Government regulation**
  - U.S. Patriot Act
  - California Anti-Hacker Legislation: SB1386
  - Graham-Leach-Bliley Act
  - FTC sues Guess.com for database compromise

- **Credit card regulations**
  - Liability shift regulations
    - Verified by Visa – new interchange pricing
    - MasterCard SecureCode
  - Network and data security regulations (impacts all processors)
    - Visa CISP (cardholder information security program)
    - MasterCard SDP (site data protection)
  - Six figure hacking penalties for non-compliance

How Fraud Happens

All payments fraud is based on stolen identities and access to payment networks

- **Stolen Consumer Identities**
  - Physical world access: Receipts, skimmers
  - Virtual world access: DB hacking, data validation, generators, black market
- **Stolen Business Identities**
  - Physical world access: Password sticky notes, poor building security
  - Virtual world access: Misconfigured web servers, log-in spoofing, black market
- **Access to Payments Networks**
  - Web based checkout page
  - Merchant account takeover

How Fraud Happens

Broadly speaking, payments fraud falls into 3 categories of theft

Category	Description	Est. $$ Impact Per Event
Product/Service Theft (Virtual Shoplifting)	▶ *Begin* with stolen consumer identities ▶ Product purchased for resale or personal use ▶ Merchant required to complete crime-- fulfillment	**$1 - $1,000**
Identity Theft (Hacking/Carding)	▶ *Goal* is to steal consumer identities ▶ Database hacking– insecure DBs provide direct access to customer lists ▶ Data validation– automated attacks trick system to give up information	**$1,000 - $10,000**
Cash Theft (Account Takeover)	▶ Begin with stolen consumer AND business identities ▶ Authorization terminal used to siphon cash from one set of cards to another ▶ Greatest economic damage	**> $10,000**

How Fraud Happens

Universe of web payments fraud attacks

Cardholder

Spoof sites

- Best Buy Fraud Alert scam
- VbV Register Card scam

Auctions

- Fraudulent sellers
- Escrow scams

Merchant

Stolen Products

- Virtual shoplifting

CC Validation

- Carding
- Generating

Infrastructure Hack

- Customer Lists

Web Gateway

Merchant ID Theft

- Dictionary attacks
- Simple PW
- Crack provisioning logic

Fraudulent Applications

- Stolen MID/TID

Processor

Merchant ID Theft

- Stolen MID/TID

Infrastructure Hack

- Straight into processor
- Direct connect software
- Trxn Files

Issuing Bank

Fraudulent Applications

- Stolen consumer identity
- Fabricated identity

Acquiring Bank

Fraudulent Applications

- Stolen merchant identity
- Fabricated identity

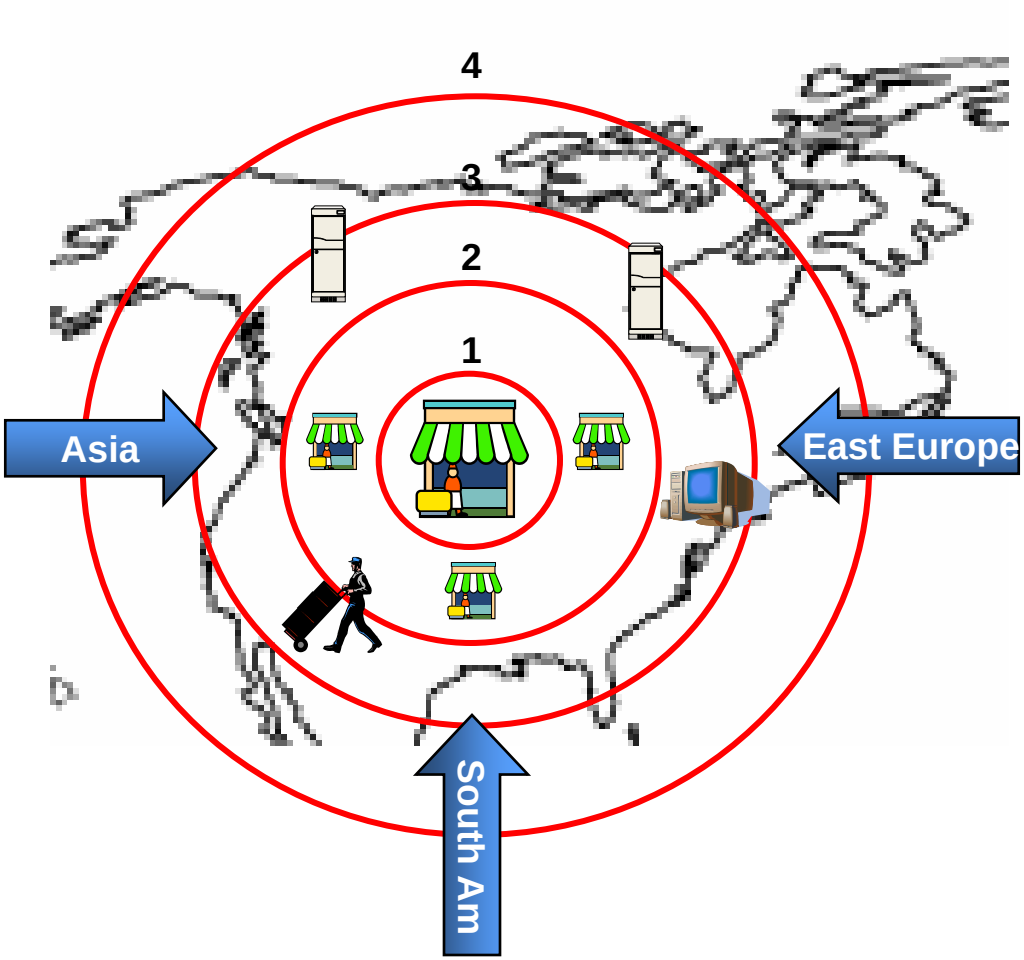
Protection Against Fraud

Businesses face both strategic and tactical challenges in effectively combating fraud

Challenge	Strategic Level	Tactical Level
Understanding Fraud Trends	▸ Lack broad **visibility** into ecommerce events ▸ Business **focus on retail**– not supporting security analysts	▸ Lack access to **specialized data** sources that inform decisions ▸ **Budget** for fraud operations
Choosing & Deploying Technology	▸ **Identifying right technologies** for specific fraud problems ▸ **Gauging efficacy** of anti-fraud technologies prior to deployment	▸ **Deploying and operating** specialized risk systems ▸ Updating systems
Evolving with Fraud	▸ Identifying and blocking **new patterns** before they strike	▸ **Testing new technologies** for new attack patterns ▸ Lack resources to manage "**positive feedback**" fraud operations

Protection Against Fraud

Effective fraud management requires protection from a broad scope of threats



Level 1: Internal Security

- Authentication & Access controls (internal fraud)
- Trxn and account activity monitoring
- Perimeter & data security

2: Other Business Security

- Have other business's secured customer lists?
- Have other business's provided data validation?

3: Infrastructure Security

- Compromised ISPs (email spoofs and fake site scams)
- Home zombie computers (attack launch points)
- Freight forwarders
- Anonymizing services

4: International

- Organized crime rings (Eastern Europe)
- International card issuers

Protection Against Fraud

True protection requires security solutions at 3 levels

- **Transaction Level**
  - Authenticate buyers when possible
  - Screen order content for fraud patterns
  - Manually review suspicious transactions
- **Account Level**
  - Lock down administrative access
  - Monitor account level activity for suspicious patterns
- **Network Level**
  - Lock down network access
  - Monitor network level activity for suspicious patterns
  - Update all patches on servers and operating systems

Protection Against Fraud

There is no software silver bullet– payments security requires an orchestration of technologies and processes…

Category	Technologies	Processes
Transaction Level	▶ Authentication ▶ Rules Engines ▶ Risk Scoring (neural nets)	▶ Manual review (standardized process) ▶ Risk tolerance policies ▶ Monitoring product sales trends
Account Level	▶ Strong password rules ▶ User roles/privileges ▶ Account activity logging	▶ Frequent password changes ▶ Maintain up-to-date employee access control ▶ Review transaction logs
Network Level	▶ IP Address restrictions ▶ Firewalls ▶ Port scanning	▶ Monitoring threat sites ▶ Maintaining current patches

Protection Against Fraud

Verified by Visa and MasterCard SecureCode protect card information at checkout

- **Real-time password authentication of buyers to their card issuers**

- **Technology Requirements**
  - MPI (merchant plug-in) to initiate authentication from checkout
  - Visa/MasterCard 3DSecure directories to route communication to issuers
  - ACS (access control server) for issuers to execute authentication
  - Processors (online & offline) must pass new data fields (ECI, CAVV, XID)

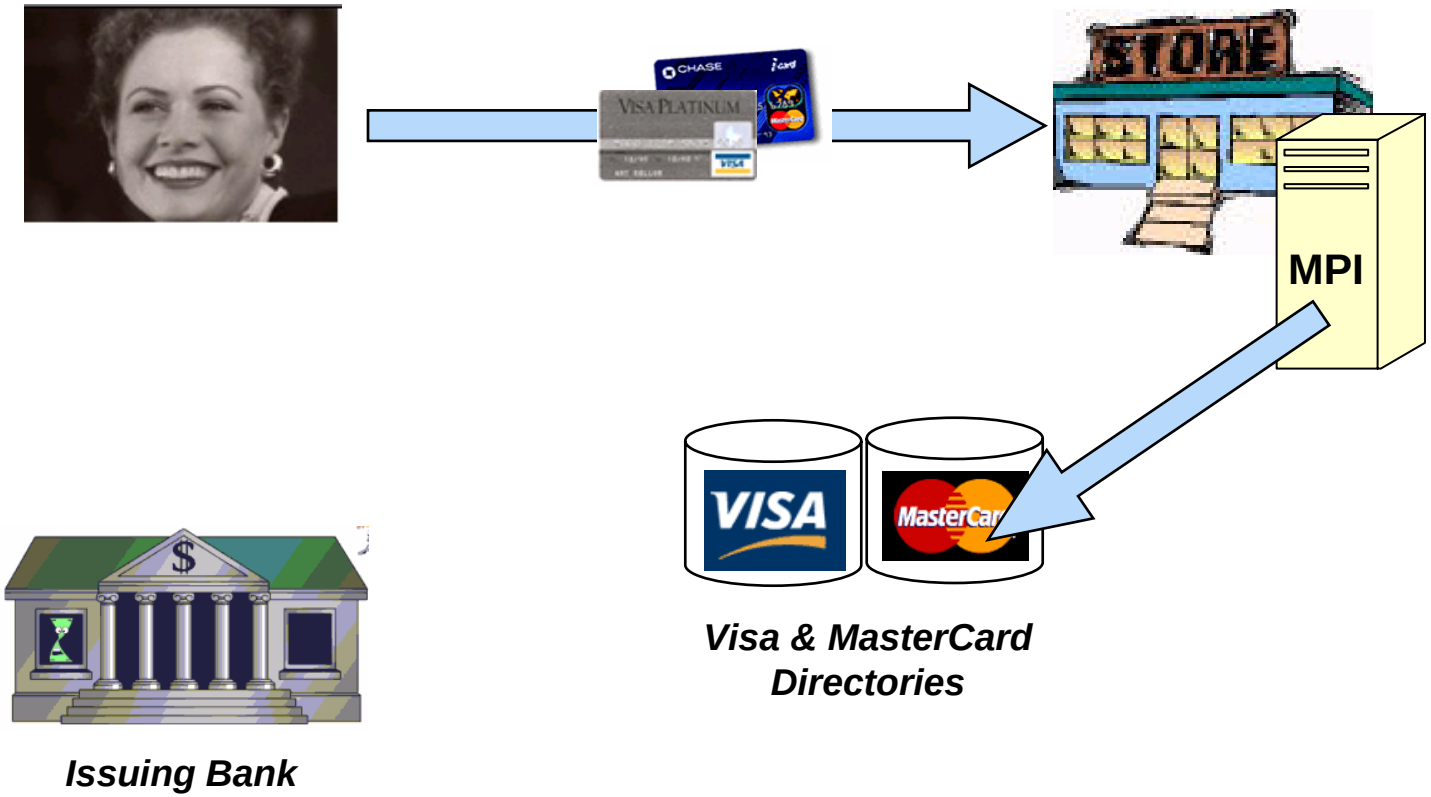
- **Limited liability protection**
  - Protects merchants from 3 Visa reason codes (23, 61, 75) and 2 MasterCard reason codes (37, 63)

Visa & MasterCard DO NOT advocate authentication as complete fraud protection!

Protection Against Fraud

How it works

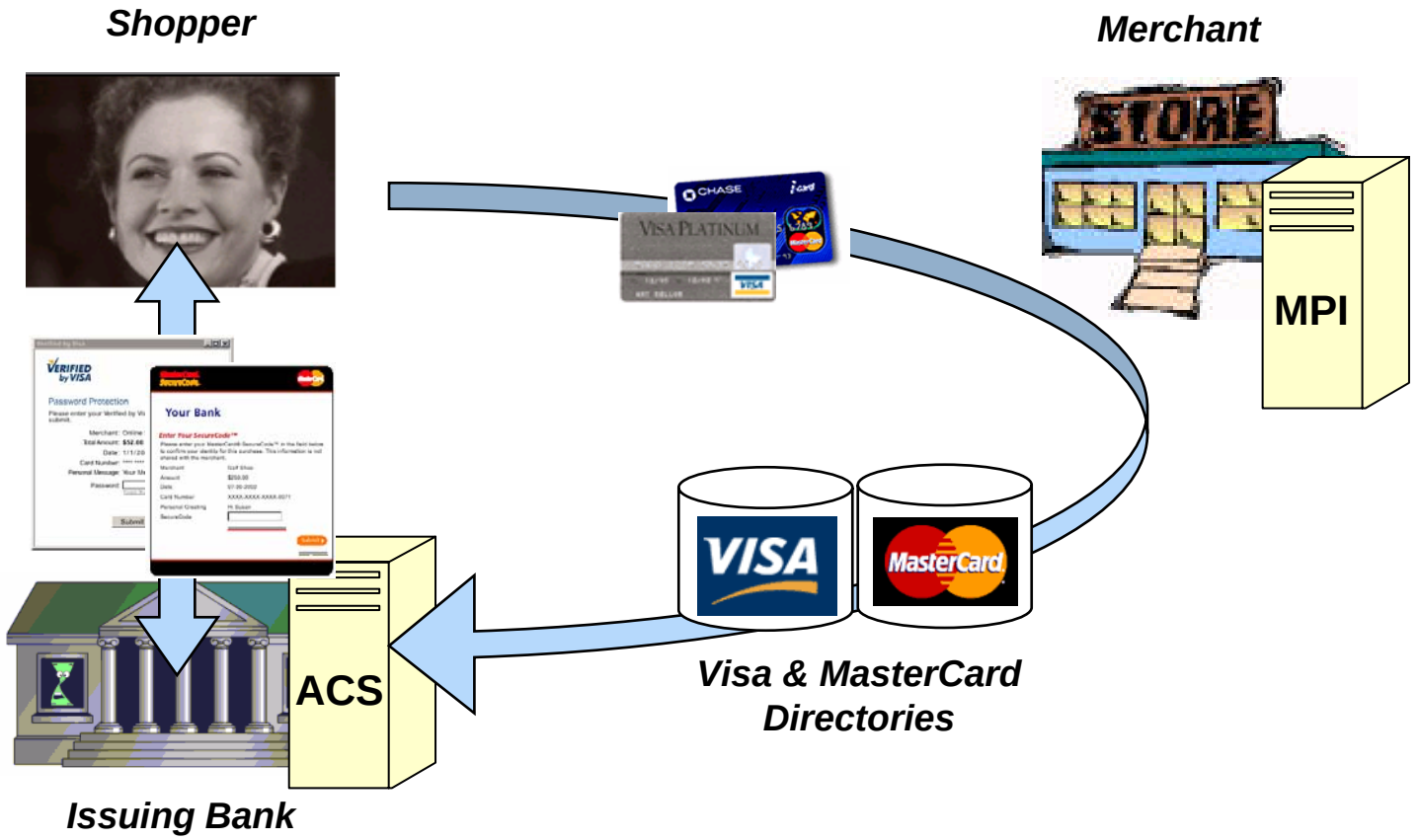
1. Consumer fills out checkout page, submits payment information to merchant
2. Merchant MPI checks Visa & MC directories for enrolled cards



Merchant Liability for Fraud

How it works

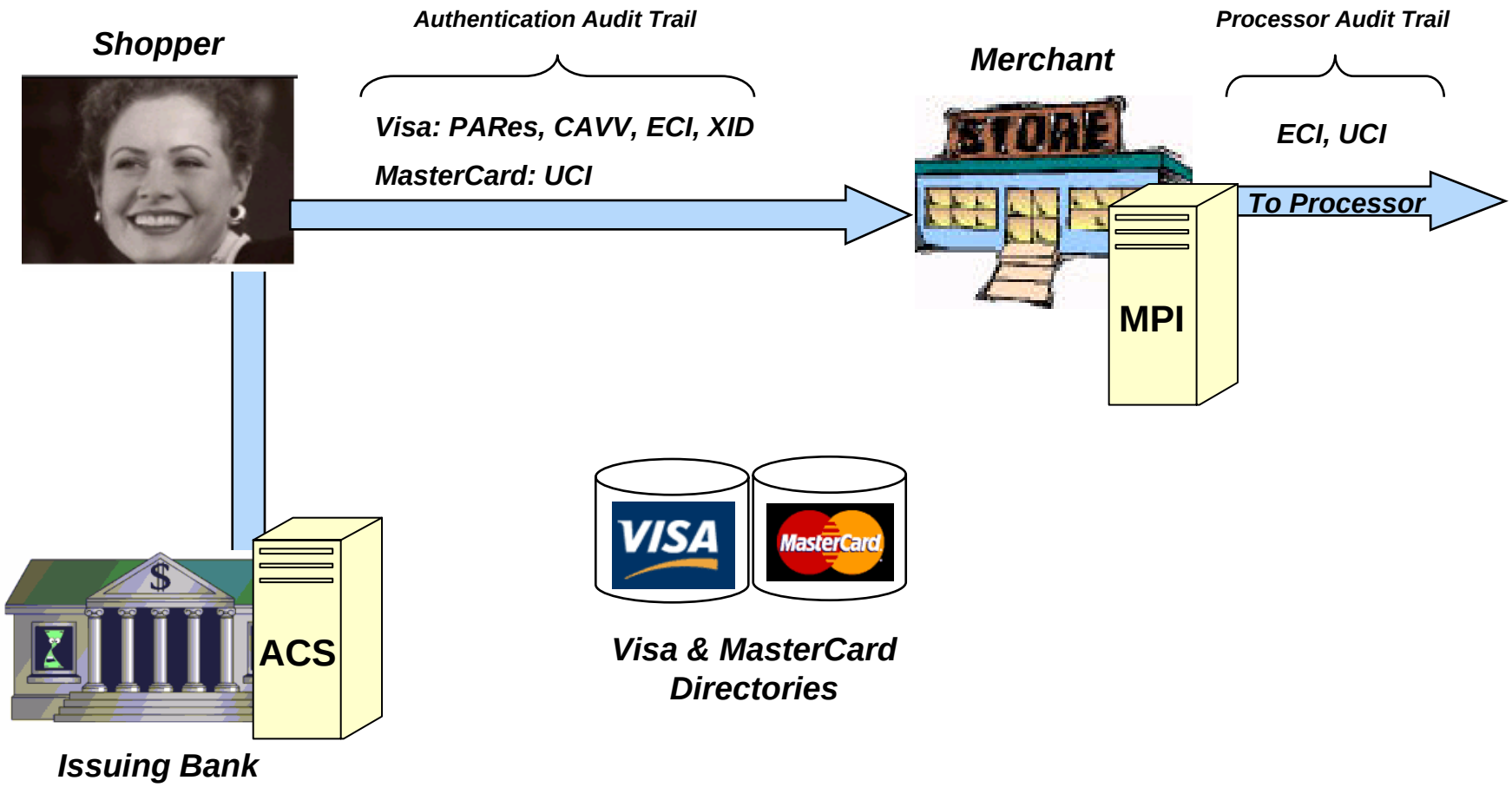
3a. For non-enrolled cards, transaction continues to processor as usual
3b. For enrolled cards, issuer prompted to authenticate user
4b. Consumer gives password, ACS validates password



Merchant Liability for Fraud

How it works

5. Authentication results passed back to merchant, proceed to authorization



Questions