



# Visa's Approach to Card Fraud and Identity Theft

Paul Russinoff

June 7, 2007



# Discussion Topics



- Visa's Comprehensive Security Approach
  - Multiple Layers
  - Commitment to Cardholders
  - Consumer Tips
  - Protecting Cardholder Information





# Identity Theft Overview

## **Identity theft is a concern for everyone**

- Fraud is number one concern among cardholders.
- Cardholder protection is one of Visa's highest priorities.
- Visa has taken a comprehensive approach to addressing the issue.

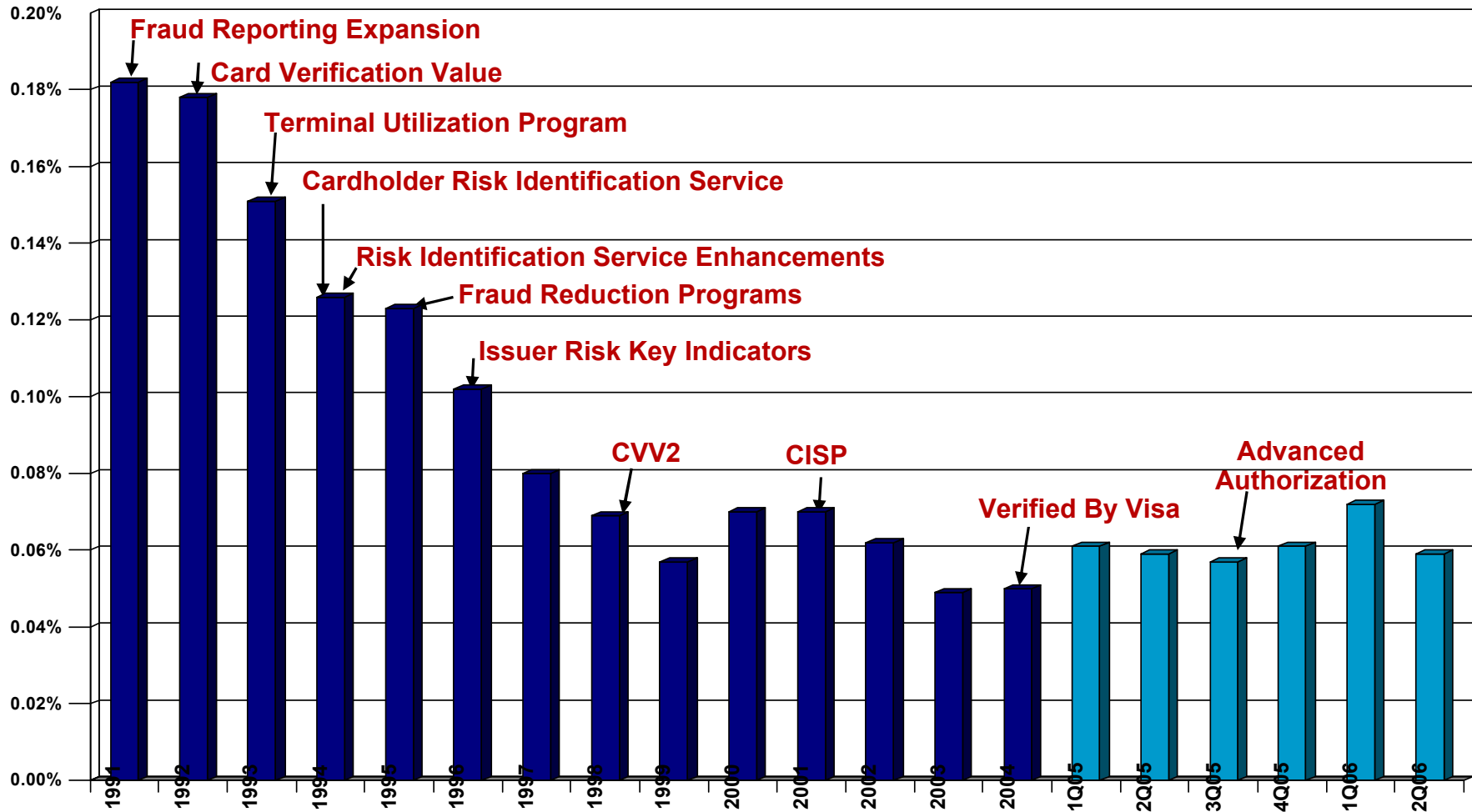
# Visa's Multiple Layers of Security



- At Visa, we are proud of our record on fighting fraud and protecting cardholder information.
  - Our goal is to actually prevent fraud from occurring in the first place.
    - We invest over \$300 million annually in the latest technologies to fight fraud.
    - Sophisticated neural networks intelligently track spending patterns.
    - “Verified by Visa” protects cardholders against e-commerce fraud.
    - Advanced Authorization instantaneously detects potential fraud occurring not only on individual cardholders’ accounts, but throughout the Visa network.
    - Cardholder Information Security Program (CISP) requires all participants in the Visa system to adhere to a set of standards for safeguarding cardholder information.
  - As a result of these and other efforts, fraud within the Visa system stood at an all-time low of just five cents per \$100 transacted as of Q3 ‘06.

# Industry Fraud Trends

## 15 Year Historical View



Net Fraud Chargeoffs As a Percent of Total Volume

Source: U.S. Member Quarterly Operating Certificates

# Visa's Commitment to Cardholders



- Should an instance of fraud actually occur, Visa's commitment to cardholders greatly minimizes the impact:
  - Our “zero liability” policy ensures that cardholders do not pay a cent for any fraudulent charges.
  - Through our partnership with Call For Action, Visa operates a toll-free hotline – 1-866-ID-HOTLINE – for Identity Theft victims.
    - Trained counselors provide free and confidential assistance, walking victims through the difficult process of getting their identities back.
    - Since the Hotline launched in April 2003, several hundred Identity Theft victims have been assisted in reclaiming their identities.
    - Visa established Personal Identity Theft Coverage that issuers can offer their cardholders
      - Ranges from \$1,000 to \$15,000 for reimbursement for lost wages, legal fees and other costs associated with recovering from an Identity Theft incident.

# Visa's Commitment to Cardholders



- Visa was the first to announce a policy of protecting consumers' identities by limiting the account information that can be printed on cardholders' receipts.
- Visa launched a campaign against phishing – another form of identity theft – in partnership with the Better Business Bureau, Call For Action, the Federal Trade Commission, and the Treasury Department.
  - Phishing is an e-mail scam in which fraudsters attempt to convince consumers to reveal personal information – such as their credit or debit account numbers, checking account information, Social Security numbers, and banking account passwords – through official-looking fake Web sites or in a reply e-mail.



# Identity Theft Tips for Consumers

- Simply monitoring your credit card and account statements on a weekly basis can greatly decrease your identity theft risk.
- Report lost or stolen credit cards immediately.
- Cancel all inactive credit card accounts.
- When using your credit card do not volunteer any personal information.
- If you've applied for a credit card and have not received the card in a timely manner, immediately notify the appropriate financial institution.
- Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to your credit card's expiration date.
- Sign all new credit cards upon receipt.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.
- Order a free copy of your credit report each year.

# If it Happens to You



- **Step 1:** Call for free, confidential counseling
  - 1-866-ID-HOTLINE
- **Step 2:** Contact credit bureaus
- **Step 3:** File a police report
- **Step 4:** Contact your creditors' fraud departments
- **Step 5:** File a complaint with the Federal Trade Commission (FTC)



# Protecting Cardholder Information: CISP and PCI

## Standard of due care and enforcement for protection of sensitive consumer information

- Visa Cardholder Information Security Program (**CISP**)
- Payment Card Industry (**PCI**) Data Security Standard
- CISP compliance required since June 5, 2001
  - All Members, merchants, and service providers that store, process, or transmit cardholder data
- Member financial institutions must use, and are responsible for ensuring that their merchants use, service providers that are CISP-compliant
- In December 2006, Visa announced a \$20 million program designed to further merchant compliance with PCI.
- Program is first of its kind to use a unique combination of incentives and fines.



# Protecting Cardholder Information: CISP



Cardholder Information Security Program	
Build and Maintain a Secure Network	<ol style="list-style-type: none"><li>1. Install and maintain a firewall configuration to protect data</li><li>2. Do not use vendor-supplied defaults for system passwords and other security parameters</li></ol>
Protect Cardholder Data	<ol style="list-style-type: none"><li>3. Protect stored data</li><li>4. Encrypt transmission of cardholder data and sensitive information across public networks</li></ol>
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"><li>5. Use and regularly update anti-virus software</li><li>6. Develop and maintain secure applications</li></ol>
Implement Strong Access Control Measures	<ol style="list-style-type: none"><li>7. Restrict access to data by business need-to-know</li><li>8. Assign a unique ID to each person with computer access</li><li>9. Restrict physical access to cardholder data</li></ol>
Regularly Monitor and Test Networks	<ol style="list-style-type: none"><li>10. Track and monitor all access to network resources and cardholder data</li><li>11. Regularly test security systems and processes</li></ol>
Maintain an Information Security Policy	<ol style="list-style-type: none"><li>12. Maintain a policy that addresses information security</li></ol>

# Comprehensive Security Approach Cardholder Protection

