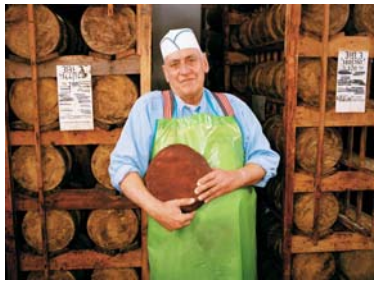
Cardholder Data Security and Fraud Prevention

Security: A Customer POV

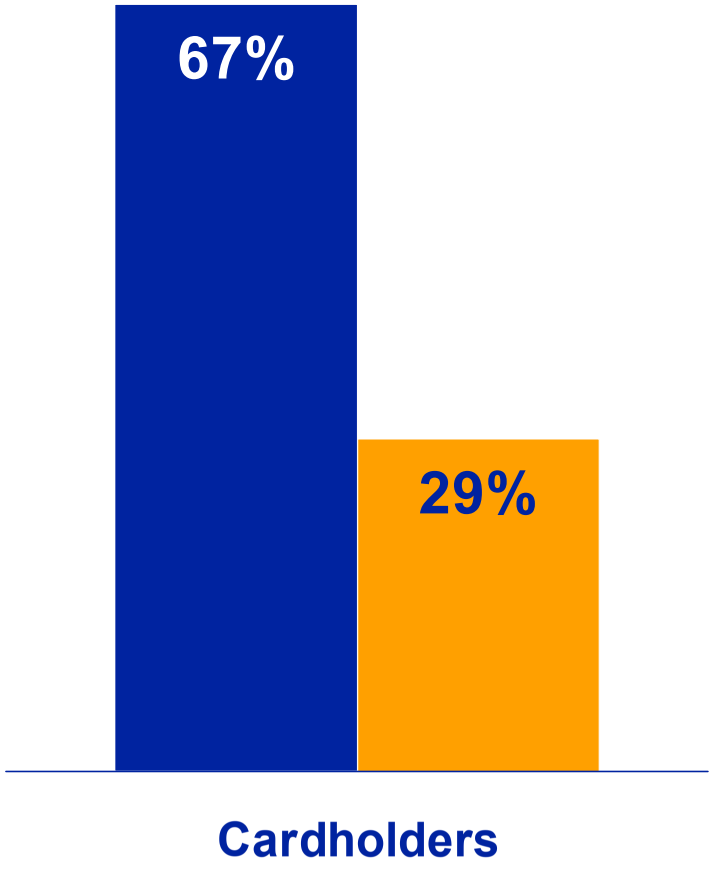




1. Cardholder awareness of security issues at **record high levels.**

2. Concerns permeate all facets of their financial life and could **impact their spending** at the checkout line.

3. **Maintaining consumer confidence** in electronic payments is mutually beneficial.

Cardholder Concerns



67% Worried

Cardholders **will be more cautious** how and where they use their credit cards in the future.

29% Not Worried

Cardholders say they **don't worry too much**. They will continue to use their credit cards as they have in the past.

Importance of Data Security for Businesses

1. Damaged reputation to your brand
2. Potential loss of consumer good will
3. Financial liability for fraud/chargebacks
4. Fines and penalties
5. Potential legal liability

Security Environment

- **Hackers are attacking:**
  - Brick-and-mortar merchants
  - E-commerce merchants
  - Processors and Agents

- **Hackers are looking for:**
  - Software that stores sensitive cardholder data
  - Personal information to perpetrate identity theft
  - Track data and payment account numbers

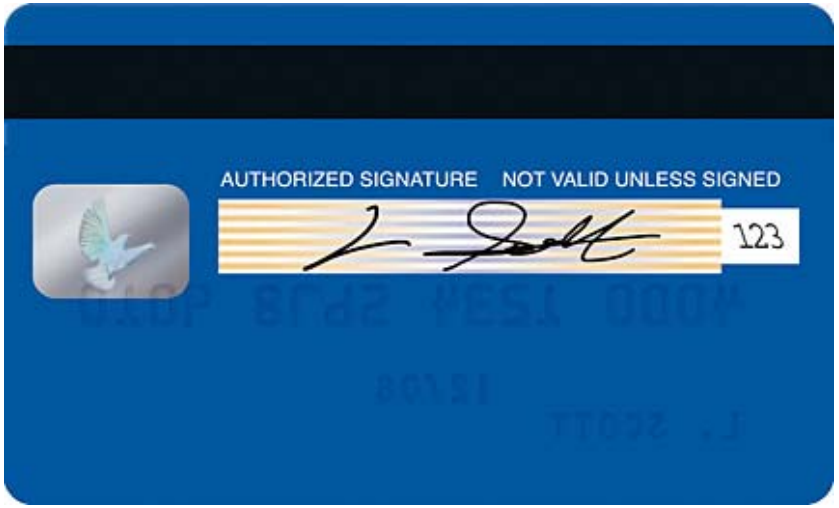
Is Your Business a Target?

ASK YOURSELF:

1. Is your POS terminal software based or is it connected to other computers or devices?
2. Do you have multiple systems connected with any having Internet access?
3. Do you have wireless access points?
4. Do you have an e-commerce component of your business?

- **If you said yes to any of these questions, you may be a target for data thieves.**
- **If no, you still may be the victim of a criminal trying to use a fraudulent card in your store.**

What the Data Criminals are After



Important, sensitive information is stored on the **card's magnetic stripe.**

If this information is stored and compromised, it can enable criminals to counterfeit cards and/or use the cards fraudulently online.

Protecting
Cardholder Data

How Businesses Can Protect Cardholder Data

Don't Store It If You Don't Need It!

1. Know exactly what you NEED to store and store ONLY that. Most businesses don't need to store any payment card data.
2. Know what your POS application is storing, if anything.
3. Know what your vendors are storing
4. NEVER store Track I or Track II data.
5. NEVER store PIN data.

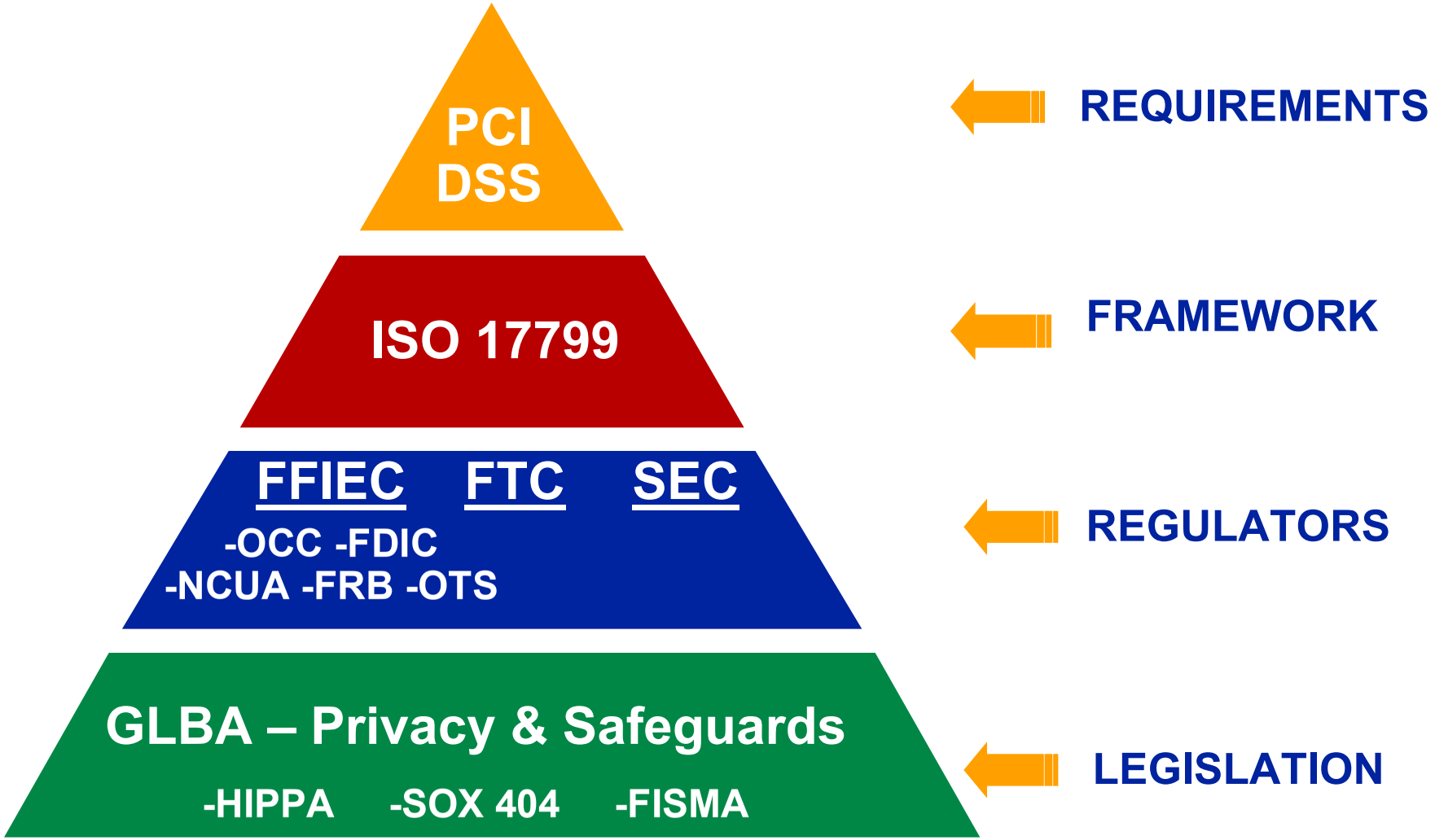
How Businesses Can Protect Cardholder Data

1. Protect cardholder receipts.

2. Know what payment application(s) you use and make sure they are not storing inappropriate data.

3. Be aware of how the Payment Card Industry Data Security Standard (PCI DSS) applies to you.

Data Security Requirements at Multiple Levels



PCI Data Security Standard

Build and Maintain a Secure Network	▪ Install and maintain a firewall confirmation to protect data ▪ Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	▪ Protect stored data ▪ Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	▪ Use and regularly update anti-virus software ▪ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	▪ Restrict access to data by business need-to-know ▪ Assign a unique ID to each person with computer access ▪ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	▪ Track and monitor all access to network resources and cardholder data ▪ Regularly test security systems and processes
Maintain an Information Security Policy	▪ Maintain a policy that addresses information security

Merchant Compliance Levels

Merchant Level 1	Any merchant processing over 6,000,000 Visa transactions per year, or identified by any other payment card brand as Level 1.
Merchant Level 2	Any merchant processing 150,000 to 6 million Visa e-commerce transactions per year.
Merchant Level 3	Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per year.
Merchant Level 4	Any merchant processing less than 20,000 Visa e-commerce transactions per year, and all other merchants processing up to 6 million Visa transactions per year.

Merchant Compliance Validation

Level	Validation Action	Scope	Validated By
1	• Annual On-site Security Audit	• Authorization and Settlement Systems	• Independent Assessor or Internal Audit if signed by Officer of the company
	• Quarterly Network Scan	• Internet Facing Perimeter Systems	• Qualified Independent Scan Vendor
2 and 3	• Annual Self-Assessment Questionnaire	• Any system storing, processing, or transmitting Visa cardholder data	• Merchant
	• Quarterly Network Scan	• Internet Facing Perimeter Systems	• Qualified Independent Scan Vendor
4	• Annual Self-Assessment Questionnaire	• Any system storing, processing, or transmitting Visa cardholder data	• Merchant
	• Network Scan Recommended	• Internet Facing Perimeter Systems	• Qualified Independent Scan Vendor

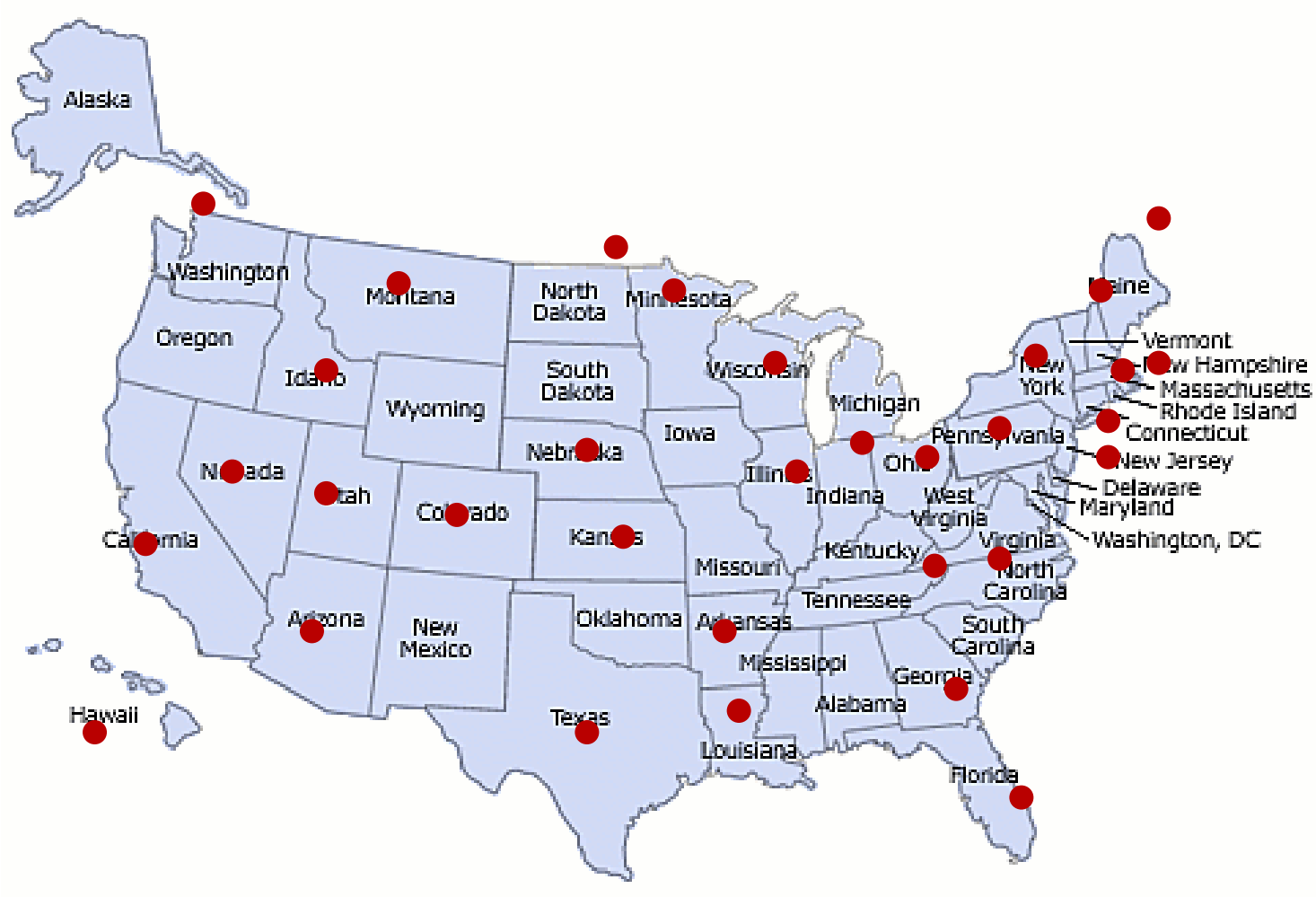
Top 5 PCI DSS Violations

Based on compromises of cardholder data, Visa has found the following common issues:

1. Inappropriate data storage (e.g., full track, CVV2, PIN blocks)
2. Un-patched systems
3. Vendor default settings and passwords (e.g., unsecured wireless)
4. Poorly coded web-facing applications resulting in SQL injection
5. Unnecessary and vulnerable services on servers

Merchants May Be Required to Notify Customers of a Data Compromise

States with 'Notice of Security Breach' Legislation

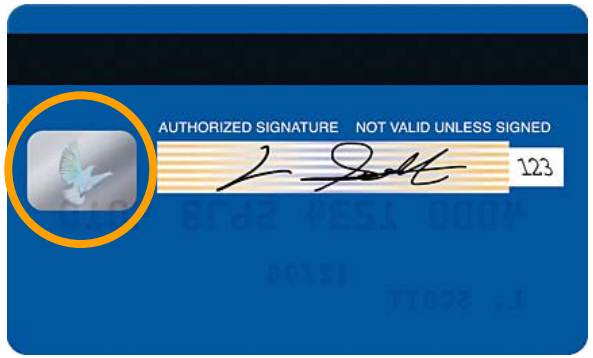


Preventing
Payment Card Fraud

Merchant Fraud Prevention

At the checkout line

Look at the card	Match receipt with card	Liability
• "Flying Dove" hologram	• The name, account number and signature on the receipt should match the card. • Merchants can ask for identification, but may not make providing it a condition of the sale.	• In face-to-face transactions, merchants are not liable for fraud when the transaction is properly authorized, which includes getting an electronic authorization. This represents the vast majority of Visa transactions.



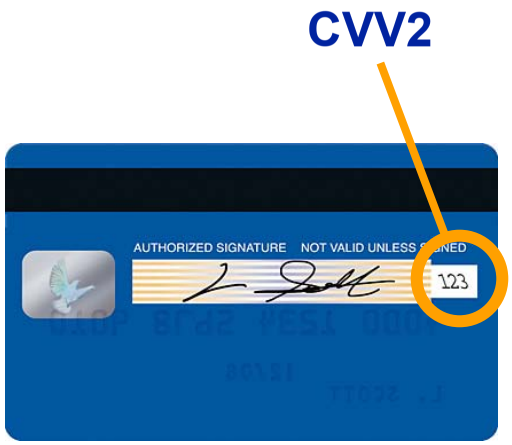
Merchant Fraud Prevention

For Internet/Catalog Sales

Authenticate the Card

CVV2

- The three-digit code printed on the signature panel, helps internet merchants verify their customers have the actual card in their possession.



Authenticate the Cardholder

Address Verification Service

- A fraud prevention system that allows merchants to compare the billing address of the purchaser with the billing address on file with the card issuing financial institution.

Verified by Visa

- A cardholder authentication service, to help online merchants reduce fraud. Participating merchants are **not** liable for certain fraudulent transactions that make up roughly 70% of online fraud.
- For more information visit **www.visa.com/verifiedmerchants**

Liability

Liability

- Merchants may be liable for card not present fraud.

Employee Fraud — Skimming

- Skimming is an illegal act that helps criminals obtain card account information to produce counterfeit cards.
- Typically, someone in the workplace uses a small device to steal information from a card's magnetic stripe. That information is put onto a counterfeit card and used to make fraudulent purchases.
- Skimming devices are small, portable – not much bigger than a pager or cell phone.
- Visa will pay a reward of **up to $1,000** for information leading to the arrest and conviction of anyone involved in the manufacture or use of counterfeit cards.

Visa Helping to Reduce Fraud

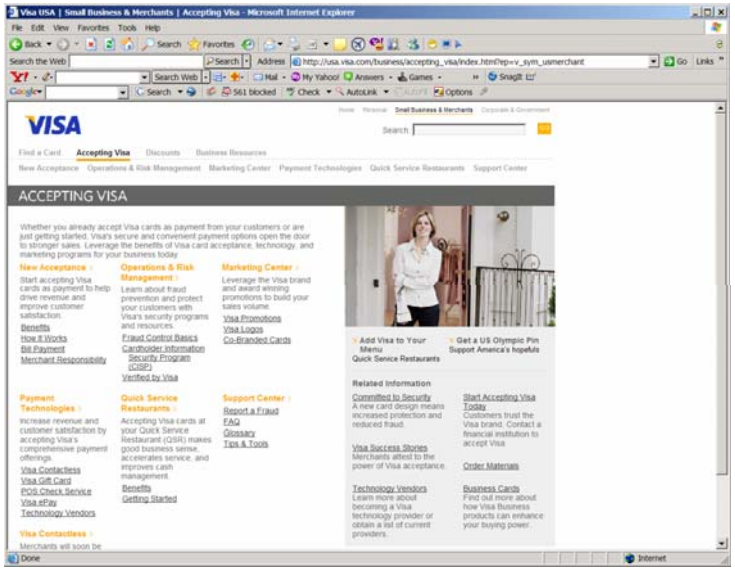
New Anti-Fraud Technology

- Visa has **cut merchant and acquirer fraud losses** by more than **$540 million** through our Resolve Online (ROL) technology which streamlines the chargeback process.
- Visa **Advanced Authorization** gives all Visa cardholders, merchants and financial institutions powerful, new fraud protection that is estimated to prevent **$164 million in fraud losses over the next five years.**
- Visa now exploring **next-generation authentication solutions.**
- Announcements will be made soon.

For More Information

Contact
your acquiring institution

Visit www.visa.com/usmerchant



Visit www.visa.com/CISP