

# Payment Card Industry Seminar

Mmm...Donuts!



Please help  
yourself to a  
donut.

Kurt Hagerman

CISSP, QSA

Director of IT Governance  
and Compliance Services



# Agenda

- Session 1: An Overview of the Payment Card Industry
- Session 2: Self Assessment Questionnaire and PCI Scans
- Session 3: Application Security
- Q & A

# *Terminology*

What is the PCI DSS FAQ for SAQ's (aka. ASA)?

When does the PABP become the PA-DSS, and is it still part of the CISP or is it now run by the PCI SSC?

How do you search for CVV2 or PAN in your CDE?

# Trends in IT Security

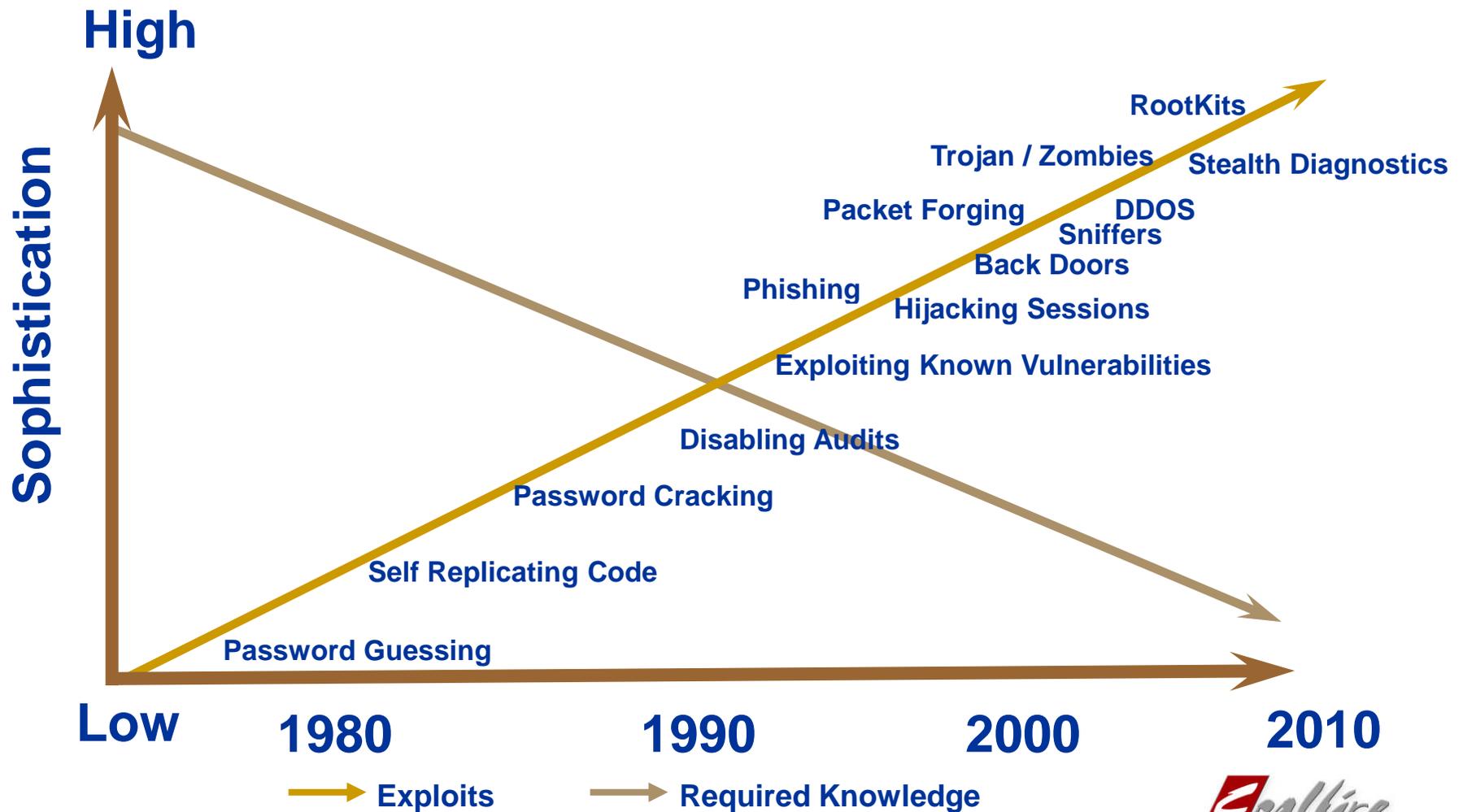


**Cash = \$10,000 to \$100,000**



**Identity Theft/Fraud = \$\$\$ Millions**

# *Its getting easier*



# Recent Data Breaches

[www.privacyrights.org](http://www.privacyrights.org)

**21 Breaches during November, 17 Breaches during December  
2 Breaches so far in January**

9-Nov-08	City of Charlottesville (Charlottesville, NC)	Two laptops containing voter registration information were stolen from a building in Charlottesville sometime after the polls closed. The information on the computers included names, addresses, date of birth and DMV customer number.	25,000
12-Nov-08	Pinellas County and Florida State agency offices	Documents with Social Security numbers, medical information and other legally protected data were found in trash containers at government buildings. Also found were hundreds of improperly discarded records were found that included medical data, privileged communications between attorneys and clients, juvenile defendant records and child abuse materials.	Unknown
2-Dec-08	Florida Agency for Workforce Innovation (Tallahassee, FL)	Employment information and more than a quarter million Social Security numbers were posted online. The breach occurred when several thousand Excel and text files containing millions of employment records were posted in the course of developing a new website.	259,193
2-Jan-09	Pepsi Bottling Group (Somers, NY)	A portable data storage device, which contained personal information, including the names and Social Security numbers of employees in the US is missing or stolen.	Unknown

# Not Just Credit Cards

```
[08:02] <Cyborgor> I CAN CASHOUT BLOCKED EGOLD.FEE DEPENDS ON BALANCE.I WILL ALSO BUY AND IF  
UR NOT VERIFIED IM NOT PAYING 1ST!!!  
[08:02] * er1ck Selling INBOX MAILER (TEST to your inbox mail), Hacked Host  
(cPanelX+FTP Access), c99 shell For scam page. Payment E-gold.  
[08:02] <\2Legit> I Am Verified USA Confirmer/Cashier I Confirm Orders From/To  
Places And Cashout Dumps + Pin t+d's I Need Credit Card Supplier All Shares Are  
50/50% I Can Cashout USA Male And Female Cvv2's Msg Me For Deal.  
[08:02] * Quits: RuiZ147 (ruiz_147@Realunix.net-3FFEEE9D.multilinks.com) ( RealUnix.Net IRC  
Server )  
[08:02] <Xuser> Have US & Australia Fresh Fulls with DL, Accept EGOLD Only ??  
[08:02] <Gass> Selling Fresh & Virgin Us / Full Info / and / cvv2 / - Kids - n00bs  
And Bullshitters Dont Msg me !.  
[08:02] <Flander> Cashing out BLOCKED EGOLD ACCOUNTS // Fees 15% // Fast and Safe //  
Contact me  
[08:02] <xDevilx> I Am Selling US Fresh Mail List 50mb - 3$ for 1mb <> Selling Fresh USA  
Socks 2$ Each <> Selling New !Commands Bot 20$ <> Selling Inbox Mailer 5$ <> Selling UK  
Mail List Fresh & Unspammed 30k - 5$ only <> Selling USA Upn 15$ <> Have All Cardable Site  
, Tested .. Ask Me For What u Want - 1$ Only <> Selling Uk Fullz With Pin - 10$ Each <>  
Selling Private Ma  
[08:02] * cintanet selling uk - us cvv fresh and valid, paypal verified (only e-gold  
and no sample tested)  
[08:02] * Quits: lux (numaro@lux.Users.RealUnix.Net) (Client exited)  
[08:02] * crazyboy im selling BANK LOGS such as AU - Anz , Suncorp , Westpac,  
Commonwealth - Uk - Natwest,LLOYDS,Halifax,Co-Operative , Ca - Desjardins prices  
in $ depends of country log u buy for more msg.me longtalkers and idiots dont  
bother!
```

# Compromise Trends



Visa “notable increase in compromise activity for 2007”

1. 83% of compromises are **small merchants** (Level 4) (represent 32% of transactions)
2. Brick and mortar compromises involving **full track data** account for the majority of exposed accounts
3. Majority of compromise incidents involve use of vulnerable **payment applications**
4. Unsecured **remote access** applications contribute to compromises

# Russian Hackers?



# New Threats

## Best Buy Digital Photo Frames Shipped With Virus

Electronics retailer **Best Buy** has pulled a popular brand of digital photo frames from its online and in-store shelves, following reports that many of the devices shipped with computer viruses.

The affected frames are limited to a particular size of Best Buy's own **Insignia** brand photo frames, the 10.4-inch version (model# NS-DPF10A). Best Buy spokesperson **Nissa French** said the virus was apparently introduced at some point in the manufacturing process (the devices are made in China).



**FOCUSED ATTACK:** Large-capacity hard disks often used by government agencies were found to contain Trojan horse viruses, Investigation Bureau officials warned

# Fun with Cell Phones

**SpoofCard**  
BE WHO YOU WANT TO BE

- Totally Private!
- Totally Fun!
- Totally Legal!

TRY IT NOW  
FREE SAMPLE CALL

PURCHASE MINUTES

ACCOUNT LOGIN

FREQUENTLY ASKED QUESTIONS

CUSTOMER SERVICE

FORUMS

“ SpoofCard allows me to make my calls truly private. I can display any number on the Caller ID, Record my Calls and Change my Voice. Whether for business or fun, it is inexpensive and easy to use! ”

  
PURCHASE MINUTES

  
ACCOUNT LOGIN

  
FREQUENTLY ASKED QUESTIONS

# Phishing Attacks

private Inbox | X

★ Mark Cho

Sir

I represent a top business executive. I have a very sensitive and private brief from this executive to ask for your partnership to re-profile funds over USD\$18,000,000,00.

I will give the details, but in summary, the funds are coming via a bank in western Europe, and this is legitimate transaction. You will be paid 22% for your "management/consultancy fees", if I am able to reach terms with you. If you are able to work to earn this fees, please write back immediately as and provide me with your confidential telephone number, and email address i will provide further details.

Please keep this close to your chest as much as possible, we can not afford any problem.

I look forward to it.

Regards,

Mark Cho

# *The Human Element*

On Wednesday, a man dressed as an armored truck employee with the company AT Systems walked into a BB&T bank in Wheaton about 11 a.m., was handed more than \$500,000 in cash and walked out, a source familiar with the case said.

It wasn't until the actual AT Systems employees arrived at the bank, at 11501 Georgia Ave, the next day that bank officials realized they'd been had.

<http://www.wtopnews.com/?sid=1325660&nid=25>



# Market Prices for Data

Boa Factory - fresh credit card dumps - Mozilla Firefox

Availability	Image	Description	Country	Quantity	Price	Unit Price
Available		Visa Signature (no limits)	USA	10	1490.00	149.00
Available		Visa Signature (no limits)	USA	100	9500.00	95.00
Available		Visa Purchasing	USA	10	1490.00	149.00
Available		Visa Business Debit	USA	40	1198.00	29.95
Available		Visa Business Debit	USA	100	2495.00	24.95
Available		Visa Business Credit	USA	40	1198.00	29.95
Available		Visa Business Credit	USA	100	2495.00	24.95
Available		Visa Business unsorted	USA	40	1198.00	29.95
Available		Visa Business unsorted	USA	100	2495.00	24.95
Available		MasterCard unsorted	USA	100	695.00	6.95
Available		MasterCard Gold	USA	40	1198.00	29.95
Available		MasterCard Gold	USA	100	2495.00	24.95
Available		MC Gold (balance \$20-30.000)	USA	10	995.00	99.95
Available		MC Gold (balance \$20-30.000)	USA	100	6995.00	69.95
Available		Diners Club	USA	10	1199.00	119.90
Available		Discover (Novus) unsorted	USA	40	638.00	15.95
<input type="checkbox"/> Available		Discover Platinum & Gold	USA	20	999.00	49.95
Available		AmEx unsorted	USA	50	997.50	19.95
Available		AmEx unsorted	USA	100	1495.00	14.95
Available		AmEx Corporate	USA	20	1599.00	79.95

63KB  
European and worldwide countries - December 2002.

We have a lot of databases besides which it mentioned above. From time to time we shall change and update the databases, which are accessible to free sale.

**First paid - serve first. No credits & loans.**

You can choose the dumps of one type for every order. Each order can not be less, than is specified in the table at the left.

**Visa Signature card dumps**



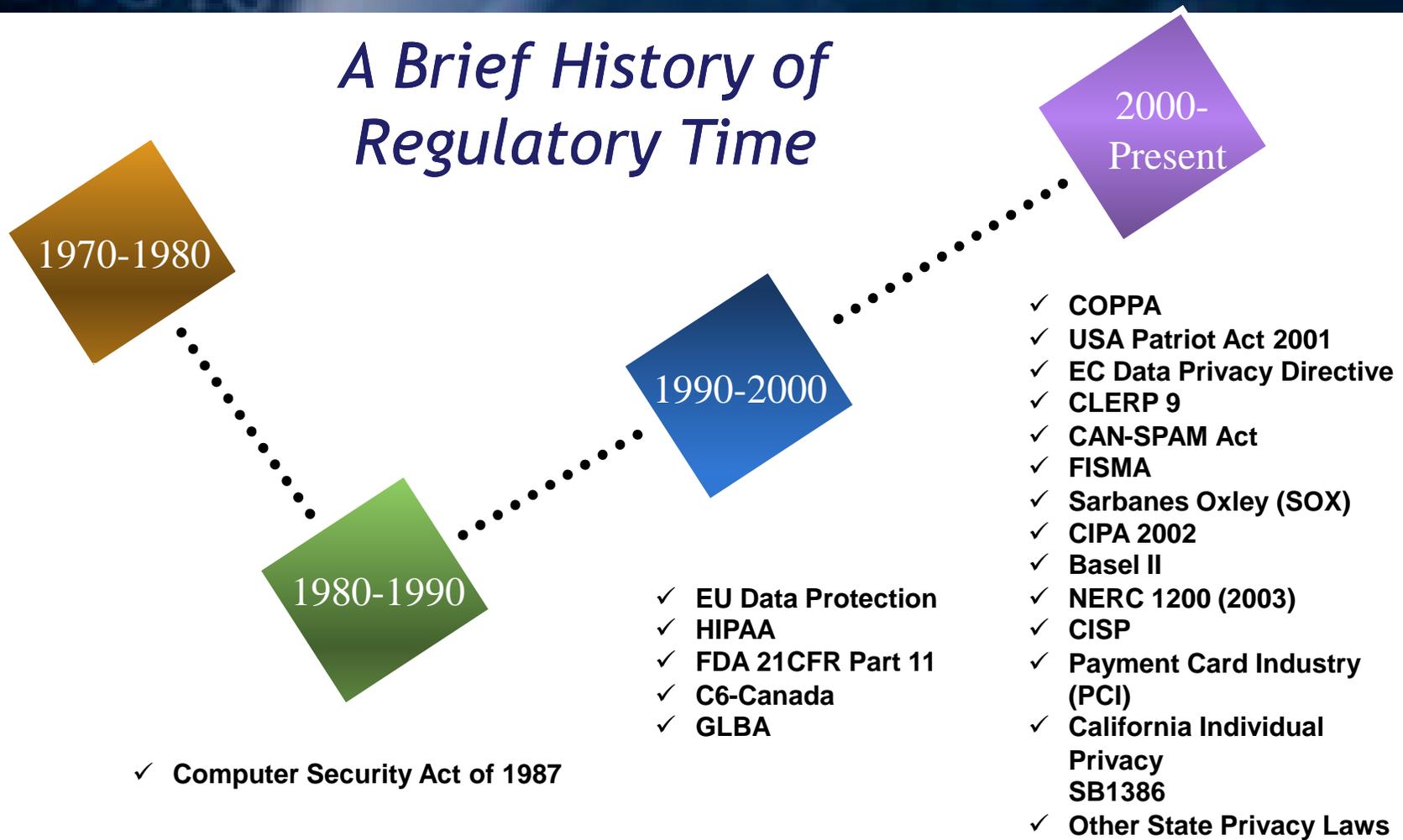
Now you can buy Visa

# *Regulatory Drivers*

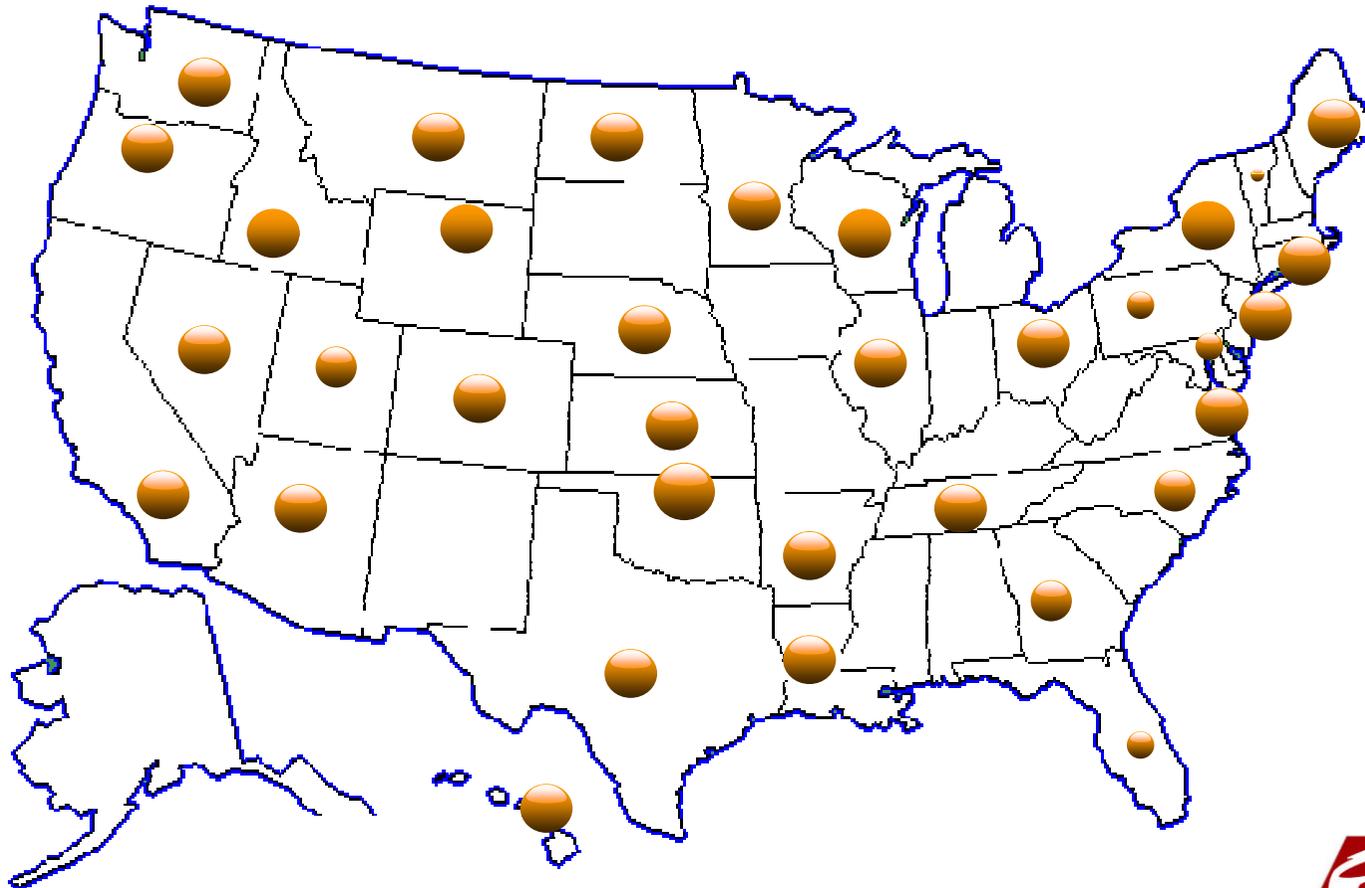
- Escalating use of e-commerce / e-government
- Rapidly escalating information breaches
- More demanding regulatory pressures
- Reduce tolerance for service disruption
- Increasing financial liability due to data breach
- Rising expectations for data privacy from citizens

# Regulatory Backdrop

## A Brief History of Regulatory Time



# *Emerging State Data Privacy Laws*



# Regulatory Backdrop

SOX

Sarbanes Oxley, passed in 2002, implements new requirements for companies that are publicly traded. Section 404 specifically concerns itself with information management, detailing IT safeguards that must be built into financial reporting.

SB  
583

Any person that owns, maintains or otherwise possesses data that includes a consumer's personal information ... and was subject to a breach of security shall give notice of the breach of security following discovery of such breach of security.

GLBA

The Gramm-Leach-Bliley Act requires protection of non-public information and personal information of customers and consumers. It established the Financial Privacy Rule, Safeguards Rule, and Pretexting Protection.

# Regulatory Backdrop

HIPAA

Passed in 2002 in reaction to the growing trend in the healthcare industry to move information online. Improving business processes and communications has great potential to improve patient care and lower costs but it may also put electronic data at risk.

FISMA

FISMA was passed in conjunction with our homeland security laws in the wake of the terrorist attacks of Sept. 11, 2001. The law has a number of security objectives, including data confidentiality, data integrity, and data availability, for government computer networks.

PCI

The major credit card companies, VISA, MasterCard, and American Express, have all initiated security programs to safeguard customer accounts and to make using credit cards online safer.



# *The Payment Card Industry*

# Who's doing what?



1. Develops Standards

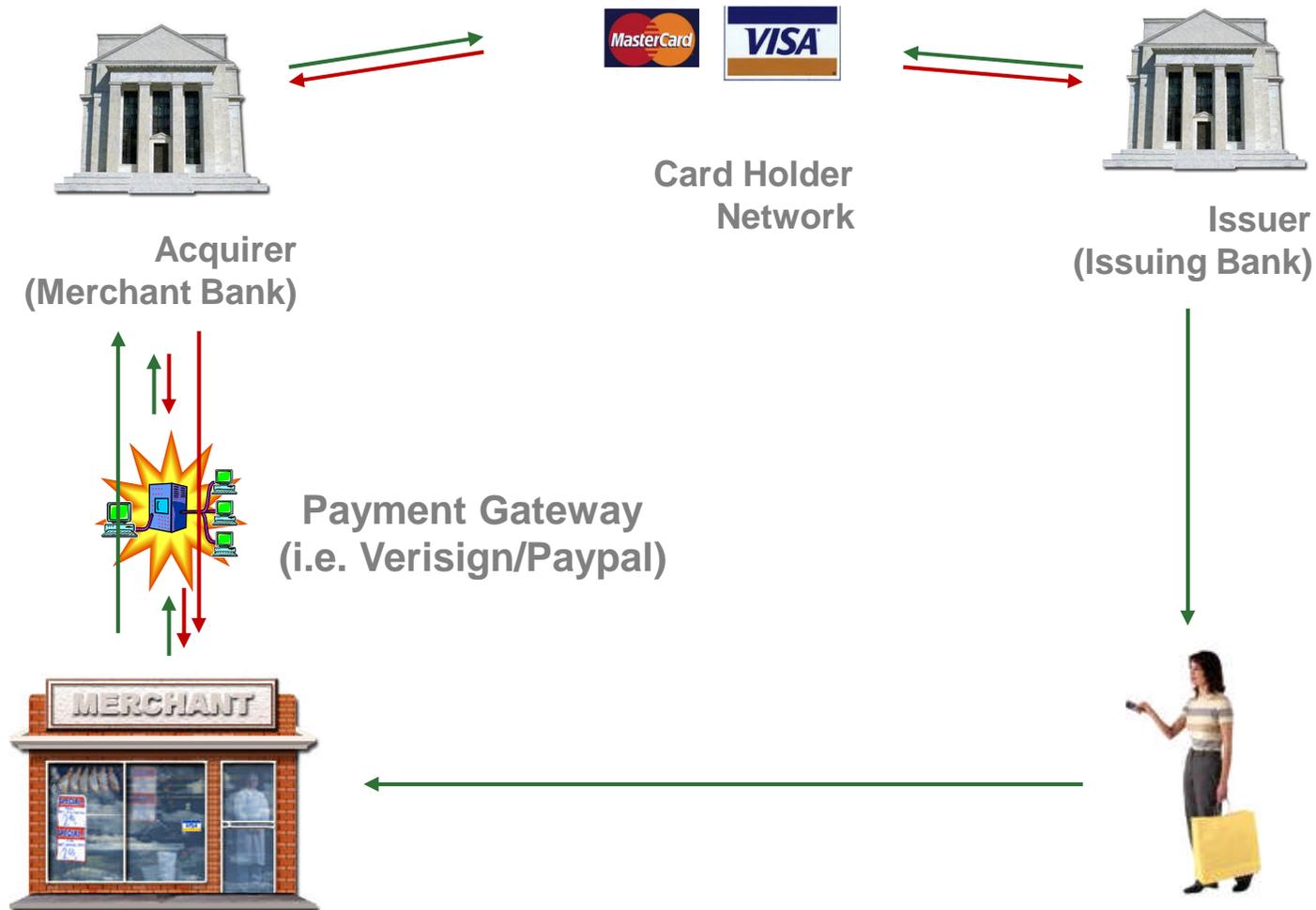


2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)

# Credit Card Processing



# Terminology

- **QSA** Qualified Security Assessor
- **ASV** Approved Scan Vendor
- **CVV2** Card Validation Value (3 Digit Number on Visa)
- **CVC2** Card Validation Code (3 Digit Number on MasterCard)
- **CID** Card Identification Data (4 Digit Number on Amex/Discover)
- **PAN** Primary Account Number
- **PABP** Payment Application Best Practice
- **CVC/CVV** Field stored on the magnetic stripe
- **Track Data** Data stored on the magnetic stripe

# What does the PCI SSC do?



1. Develops Standards

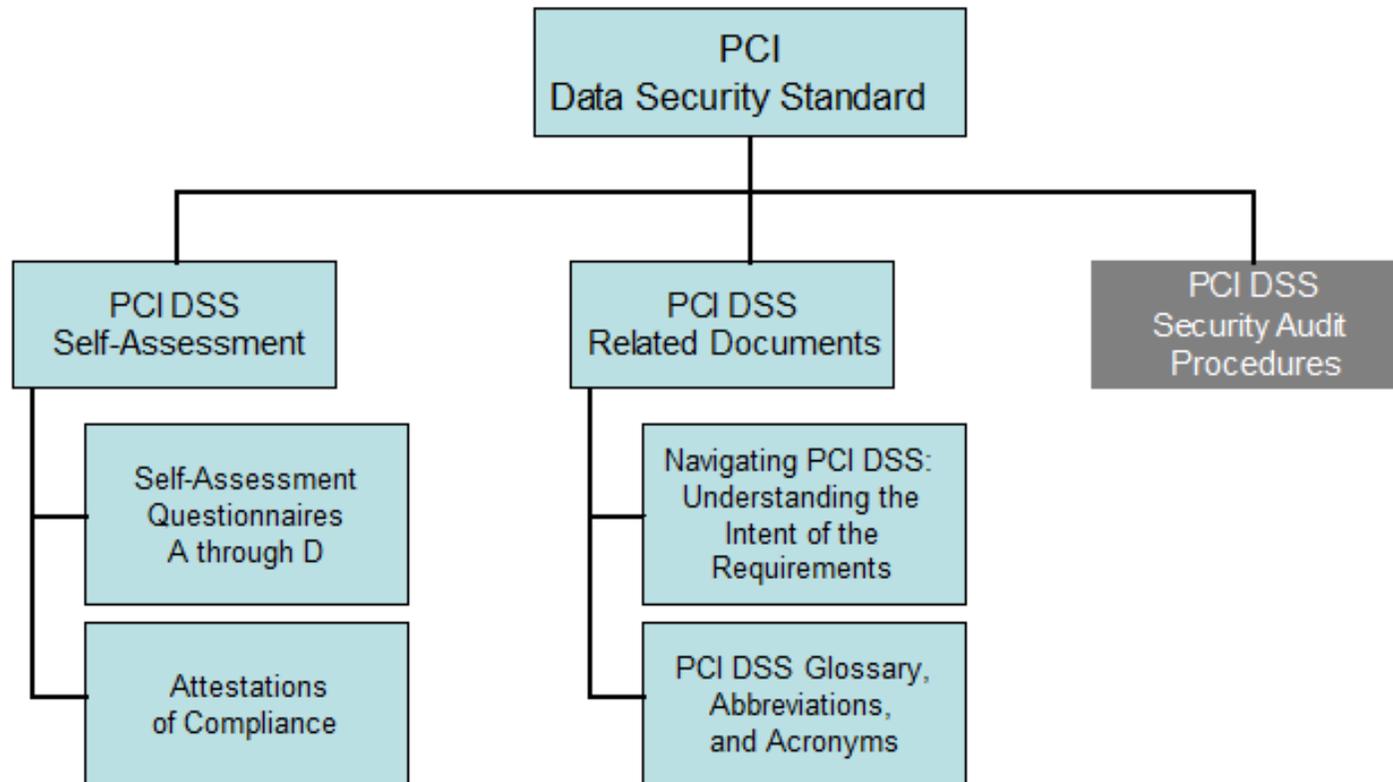


2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)

# PCI Data Security Standard



# 4 Security Standards



The screenshot shows the PCI Security Standards Council website. At the top, there is a navigation bar with links for SITE MAP, CONTACT US, PRIVACY POLICY, and TERMS AND CONDITIONS. Below this is a search bar and the PCI Security Standards Council logo. A secondary navigation bar contains links for About Us, Participation, Security Standards, Resources, Training, Programs, and News and Events. The 'Security Standards' link is circled in red and has a dropdown menu open, listing: PCI DSS, PCI DSS Self-Assessment Questionnaire, PIN Entry Devices, and Payment Application Data Security Standard (PA-DSS). The main content area features a 'Welcome to the PCI Security Standards' heading, followed by introductory text about the council's mission. Below this are two highlighted boxes: 'PCI Data Security Standard' and 'PIN Entry Devices Program'. On the right side, there is a 'JOIN NOW as a Participating Organization' button, a 'FAQs' section with a link to view frequently asked questions, and a 'Recent News' section with a headline about a webinar on the new Payment Application Data Security Standard held on May 7, 2008.

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)



# Supplemental Material



1. PCI Security Audit Procedures
2. Network Security Scan Requirements
3. Navigating the DSS
4. FAQ's for SAQ's
5. Penetration Testing Guidance
6. Web Application Firewall Guidance
7. Feedback Forms

**Payment Card Industry Security Audit Procedures and Reporting**

The document is to be used by those merchants and service providers who require an audit review to validate compliance with the Payment Card Industry (PCI) Data Security Standard and create the Report on Compliance.

Note that these PCI Data Security Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all "system components" which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and HTTP. Applications include all purchased and custom applications, including both internal and external (web) applications.

**Payment Card Industry Self-Assessment Questionnaire**

**Glossary**

**How to Complete the Questionnaire**

The questionnaire is divided into sections. The requirements included in the questionnaire are:

**Questionnaire Requirements**

The following must be included in the questionnaire:

**Organization Information**

CORPORATE NAME:  
CONTACT NAME:  
PHONE:  
APPROXIMATE NUMBER OF EMPLOYEES:  
PLEASE INCLUDE A BRIEF DESCRIPTION OF YOUR BUSINESS AND/OR INDUSTRY:  
PLEASE EXPLAIN YOUR BUSINESS NEEDS FOR THE QUESTIONNAIRE:  
LIST ALL THIRD PARTY PROCESSORS:  
Web Hosting:  
Co-Location:  
LIST POINT OF SALE (POS) TERMINALS:

**Payment Card Industry Data Security Standard**

**Build and Maintain a Secure Network**

Requirement 1: Install and maintain a firewall configuration to protect data.  
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

**Protect Cardholder Data**

Requirement 3: Protect stored data.  
Requirement 4: Encrypt transmission of cardholder data and sensitive information across public networks.

**Maintain a Vulnerability Management Program**

Requirement 5: Use and regularly update anti-virus software.  
Requirement 6: Develop and maintain secure systems and applications.

**Implement Strong Access Control Measures**

Requirement 7: Restrict access to data by business need-to-know.  
Requirement 8: Assign a unique ID to each person with computer access.  
Requirement 9: Restrict physical access to cardholder data.

**Regularly Monitor and Test Networks**

Requirement 10: Track and monitor all access to network resources and cardholder data.  
Requirement 11: Regularly test security systems and processes.

**Maintain an Information Security Policy**

Requirement 12: Maintain a policy that addresses information security.

Note that these Payment Card Industry (PCI) Data Security Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all "system components" which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and HTTP. Applications include all purchased and custom applications, including internal and external (web) applications.

Payment Card Industry Data Security Standard  
Version 1.0 November 23, 2004



# *Validation Requirements*

# What do the Card Brands do?



1. Develops Standards



2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)

# Merchant Levels

## Defined by Card Brand

Level	American Express	MasterCard	Visa
1	Merchants processing over <b>2.5 million</b> AMEX card transactions annually or any merchant that AMEX otherwise deems a Level 1.	Merchants processing over <b>6 million</b> MasterCard transactions (all channels) annually or compromised merchants.	Merchants processing over <b>6 million</b> Visa Transactions annually, identified by another payment card brand as <b>level 1</b> , or merchants compromised last year.
2	Merchants processing <b>50,000 to 2.5 million</b> AMEX transactions annually, or any merchant that AMEX otherwise deems a Level 2.	Merchants processing <b>1 million to 6 million</b> MasterCard transactions annually or any merchant considered Level 2 by another card brand.	Merchants processing <b>1 million to 6 million</b> Visa transactions annually.
3	Merchants processing less than <b>50,000</b> AMEX transactions annually.	Merchants processing over <b>20,000 MasterCard e-commerce</b> transactions annually.	Merchants processing <b>20,000 to 1 million Visa e-commerce</b> transactions annually.
4	N/A	All other MasterCard merchants.	Merchants processing less than <b>20,000 Visa e-commerce</b> transactions annually, and all other merchants processing up to <b>1 million</b> Visa transactions annually.

# What do the Bank's do?



1. Develops Standards



2. Establishes compliance requirements



3. Enforces requirements on merchants (i.e. cities)

# Merchant Validation Requirements

## Enforced by Banks

PCI DDS 11.2 requires that all merchants perform external network Scanning from an Approved Scan Vendor (ASV).

Level	American Express	MasterCard	Visa
1	<ul style="list-style-type: none"> <li>Onsite Review by a QSA.</li> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Onsite Review by a QSA.</li> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Onsite Review by a QSA.</li> <li>Quarterly Network Scan by ASV.</li> </ul>
2	<ul style="list-style-type: none"> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> <li>Quarterly Network Scan by ASV.</li> </ul>
3	<ul style="list-style-type: none"> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> <li>Quarterly Network Scan by ASV.</li> </ul>
4	N/A	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> <li>Quarterly Network Scan by ASV.</li> </ul>	<ul style="list-style-type: none"> <li>Annual Self-Assessment Questionnaire</li> <li>Quarterly Network Scan by ASV.</li> </ul>



## ***5 Keys to Success***



# 1. *Understand your Environment*

- Hannaford's Grocers – First "PCI-Compliant" merchant to suffer a significant compromise. 4.2 million records stolen. Class action law suits filed.
- Department of Veterans' Affairs Chief Information Security Officer resigned after a data breach involving more than 26 million vets
- DSW Shoe Warehouse, First time a Public Company 10Q reflected a financial loss due to a privacy violation.
- ChoicePoint, the highest profile occasion where the FTC levies fines based on references to "deceptive and unfair trade practice" associated with a Data Privacy Breach.
- HM Revenue and Customs chairman resigned after the loss of more than 25 million records on CD's.



## 2. Quantify the risks

### Compromised merchants automatically become Level 1

#### Prohibited Data (Magnetic Stripe, CVV2 or PIN Data)

Merchants are prohibited from storing full track data, CVV2 or PIN data. Under Visa's PCI CAP, fines will be assessed on acquirers for both Level 1 and Level 2 merchants who store prohibited data based on the following:

<u>PCI Level</u>	<u>Fines &amp; Fees</u>	<u>Validation Deadline</u>
Level 1	Up to \$10,000 per month (during the first three months)	<b>September 30, 2006</b>
Level 1 & Level 2 (Newly identified in 2006)	Up to \$10,000 per month for Level 1 merchants and up to \$5,000 per month for Level 2 merchants (during the first three months)	<b>March 31, 2007</b>

*Note: These fines will be escalated after three months for non-compliant merchants.*

#### PCI DSS Full Compliance

Accelerated enforcement dates for acquirers to validate full PCI compliance for Level 1 and Level 2 merchants:

<u>PCI Level</u>	<u>Fines &amp; Fees</u>	<u>Validation Deadline</u>
Level 1	\$25,000 per month	<b>September 30, 2007</b>
Level 2	\$5,000 per month	<b>December 31, 2007</b>

All fines, fees and reimbursements to card issuers levied by the card organizations against Bank of America for non compliance will be reimbursed by merchants from sources available to us.

Moreover, effective October 1, 2007, non-compliant merchants will no longer qualify for Visa's tiered interchange programs.



### *3. Understand your data*

- Know where your sensitive data is
- Keep only the data you need ... and encrypt it
- Enact strict guidelines for data access
- Set clear objectives in realistically achievable pieces
  - There is no shortage of conversation and “quick fix” solutions. Successful agencies/departments take a calm and calculated approach, steadily tackling one attainable goal at a time.



## 4. Go beyond the paper binders

The paper binder will not protect you on its own!

### Risk Analysis

- Identification
- Categorize the risks
- Remediation plan

### Prevention

- Controls
- Resources
- Training and Awareness

### Infrastructure

- Networks (Firewalls, IDS/IPS)
- Servers (Patching, AV, Controls)
- Applications (Code Review, SDLC)



## 5. Executive Sponsorship

- The most successful security programs are those which gain the interest of senior management - early on.
- Presentation of the department's current (and needed) security status to senior management.
- Insist that regular progress reports are given to the senior management.

# Key Take Aways

1. If a merchant is breached, how much will PCI SSC fine you?
2. What's the validation difference between Level 2, 3, and 4 merchants?
3. What is an ASV? QSA?
4. What the difference between the DSS and the SAQ?

# End of Session 1



**How do you manage risk?**