

Beyond PCI™

Protecting Business Assets

“IT” Data Breaches
Mitigation and Response for Financial Services

Thomas A. Layman, Ph.D.

SCAFP

Long Beach, CA

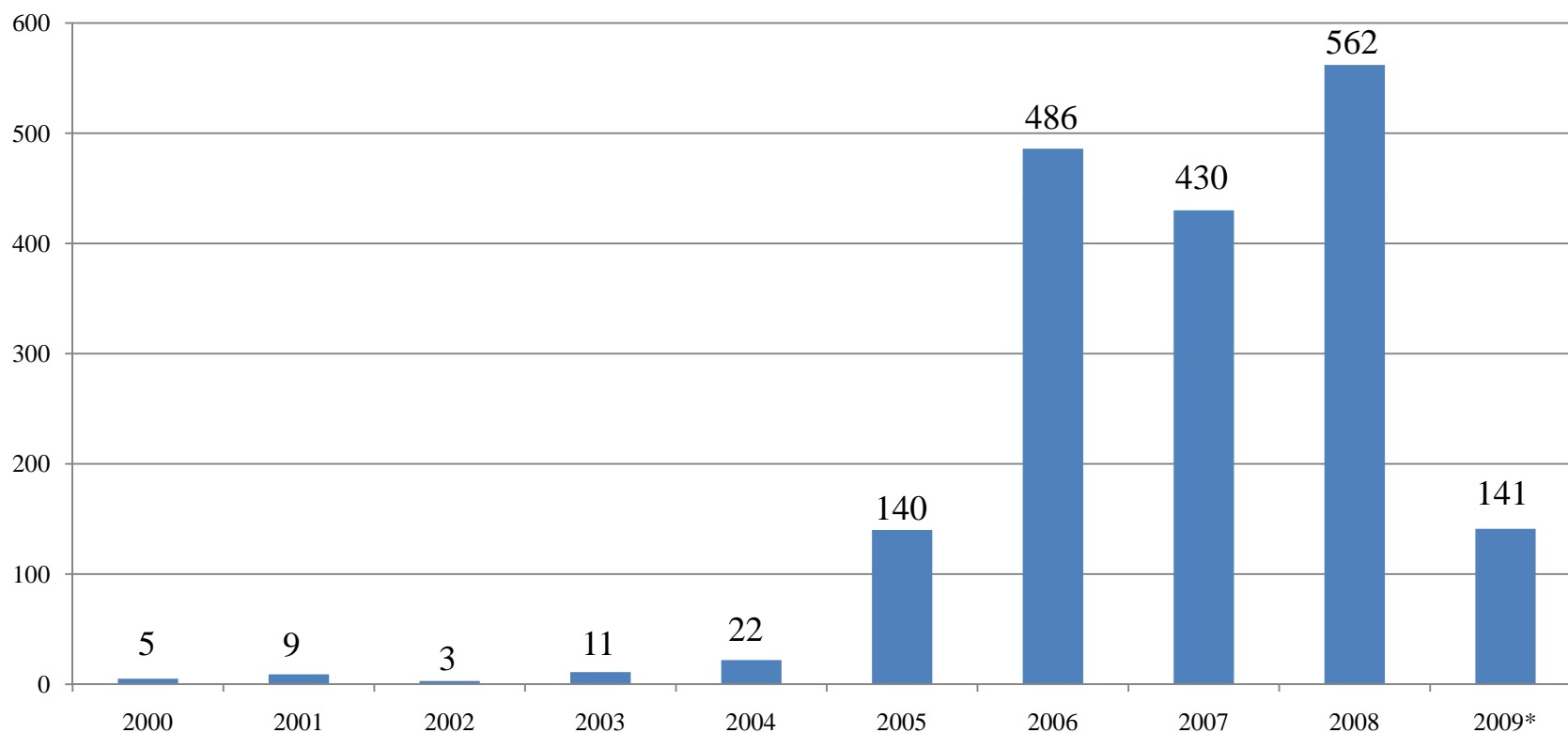
May 7, 2009

Presentation Questions

- Are data breach incidents in the US and globally a problem?
- What do you do when a breach incident occurs?
- What are the costs of a breach incident?
- What is PCI DSS?
- What is **Beyond PCI**?

Number of Global Data Breach Incidents 2000-2009*

Frequency of Event



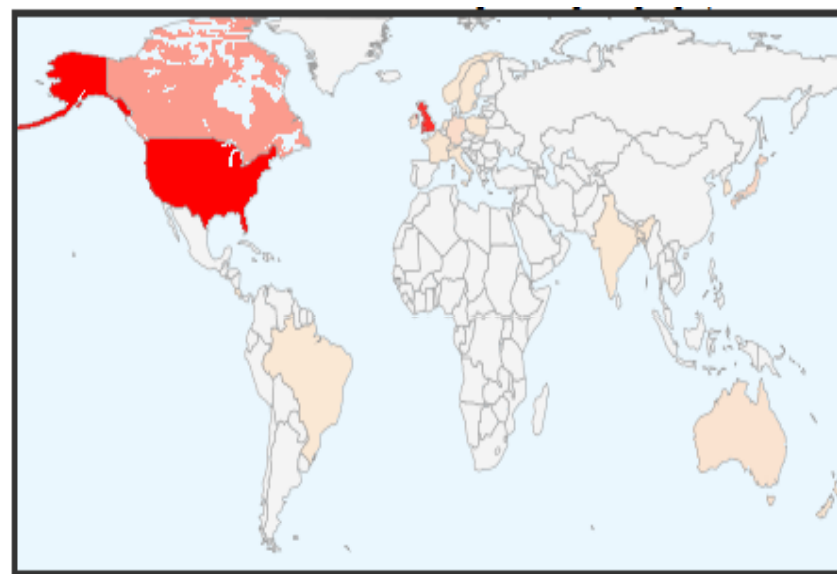
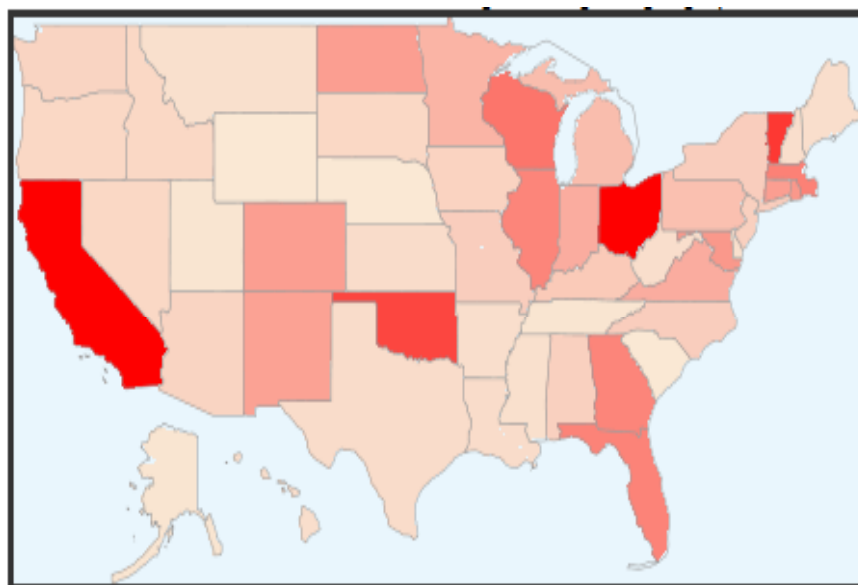
*Reported through April 3, 2009
Source: //datalossdb.org/statistics

Data Breach Incidents by Location

Incidents / HQ Location—2000-2009*

US Data Security Breaches

Global Data Security Breaches

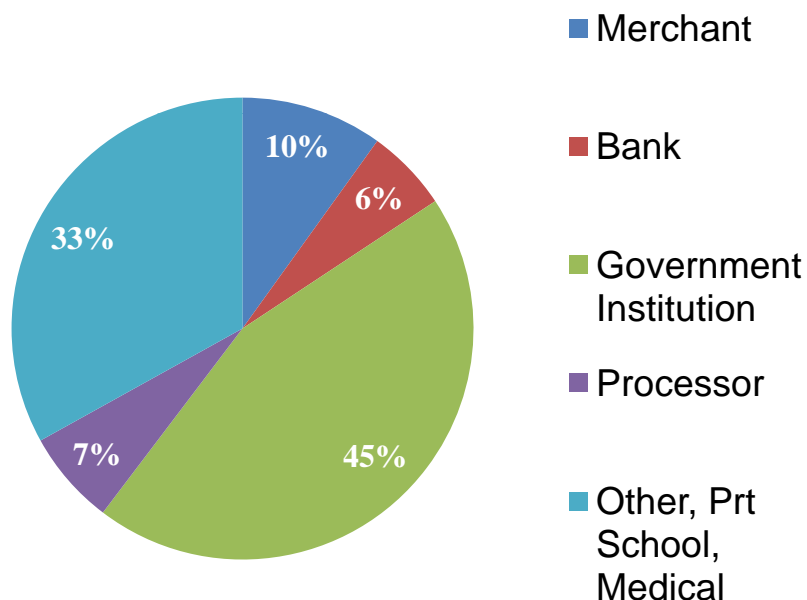


*Reported through April 3, 2009
Source: //datalossdb.org/statistics

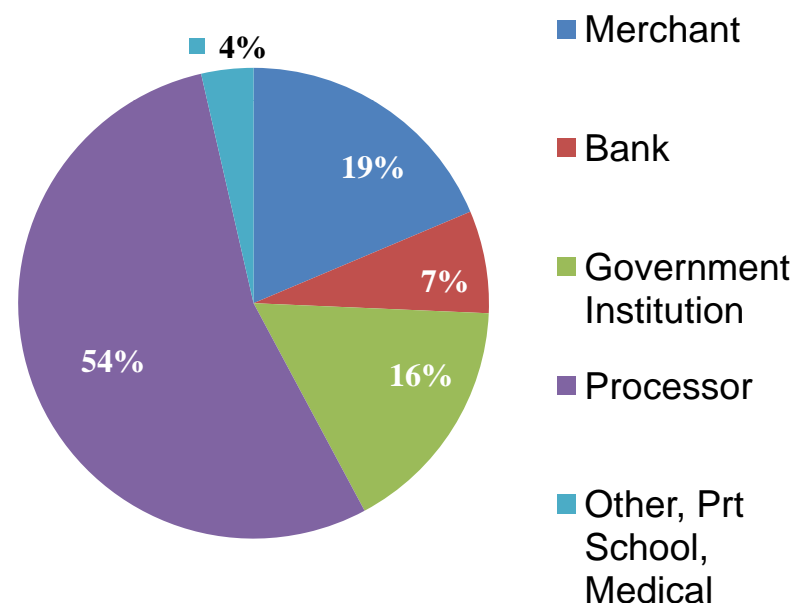
Data Breach Incidents by Type

2005-2009*

Incident Share



Number of Records Compromised



*Reported through April 3, 2009
Source: www.privacyrights.org

Largest Incident by Records Compromised 2000-2009*

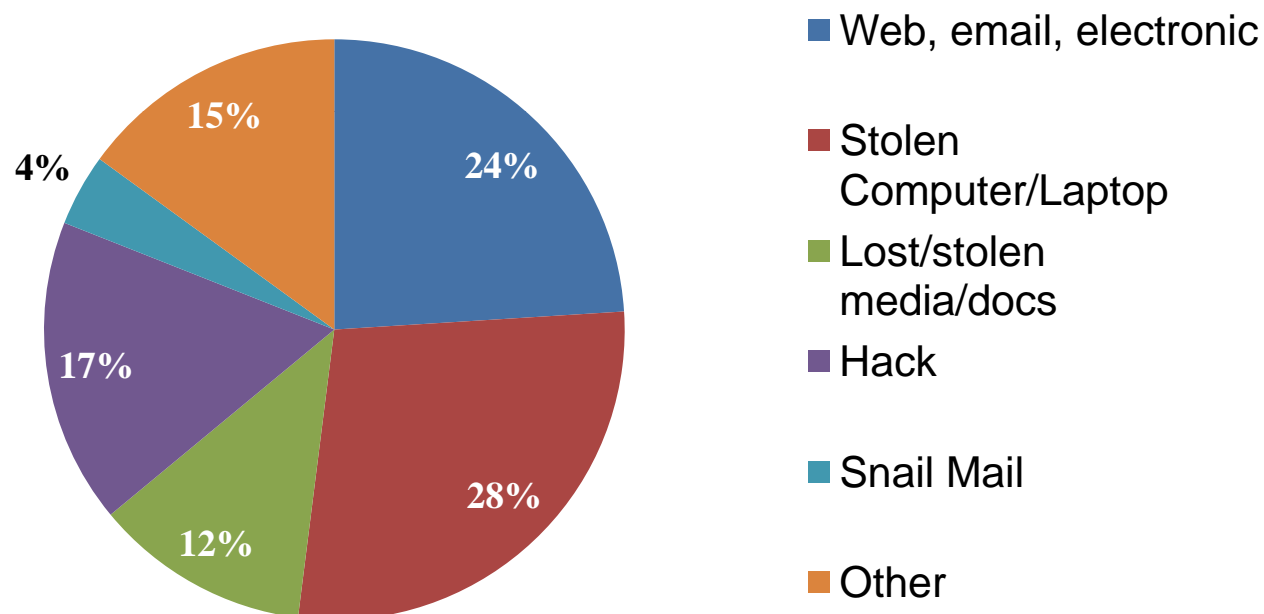
Heartland	100,000,000 ???
TJX Inc.	94,000,000
CardSystems Inc.	40,000,000
America Online	30,000,000
US Dept Veteran Affairs	26,500,000
HM Revenue & Customs	25,000,000
T-Mobile, Deutsche Telecom	17,000,000
Archive Systems, Mellon Bank NY	12,500,000
Caltex	11,000,000
Dai Nippon Printing Company	8,637,405
Certegy Check Fiserv	8,500,000
Hannaford Grocery	4,200,000
Colorado DMV	3,400,000
Countrywide Mortgage	2,000,000
RBS WorldPay	1,500,000

*Reported through April 3, 2009

Source: www.privacyrights.org//datalossdb.org/statistics

Data Breach Incidents by Source 2000-2009*

Source of Incidents



*Reported through April 3, 2009
Source: //datalossdb.org/statistics

Data Breach Notification Requirements

- Card branded networks require notification of a data breach as soon as possible after recognition
- In July 2003, California was the first state to enact legislation requiring notification of security breach
- As of July 2009, 43 states and 3 territories will have implemented notification requirements for data security breaches
 - Half require immediate notification based on the fact that information was breached or lost
 - Half use risk-based triggers, with notification based on some analysis to determine the risk of the loss
- The following 11 states/territories have not yet implemented mandatory notification of security data breaches:

Alabama	Guam	Missouri	New Mexico
American Samoa	Kentucky	Mississippi	South Dakota
Fed. State of Micronesia	Maryland	Northern Marianas	

Sources: FinancialPrivacyNow.org; www.pirg.org/consumer/credit/statelaws.htm

Cost of a Data Breach

- Estimated costs of responding to a data breach vary by industry and by the size of the data loss
- For 250,000 records, one firm estimates that the cost could range between \$10-15 million
- These estimates do not include potential lost sales/revenue and customer attrition as a result

Enter the total number of affected records here (no commas ie., 25000)		250000	
Internal Investigation	-20%	<i>Average Cost</i>	+20%
Cybercrime consulting	426806.4	533508	640209.6
Attorney fees	432744.4	540930.5	649116.6
Sum:	\$ 859550	\$ 1074439	\$ 1289327
Notification/Crisis Management			
Customer notification (certified mail)	786808.4	983510.5	1180212.6
Call center support	556704	695880	835056
Crisis management consulting	311754.4	389693	467631.6
Media management	61608.4	77010.5	92412.6
Sum:	\$ 1716874	\$ 2146095	\$ 2575314
Regulatory/Compliance			
Credit monitoring for affected customers	3577751.2	4472189	5366626.8
Regulatory investigation defense	1323470.8	1654338.5	1985206.2
State/Federal fines or fees	2807272.8	3509091	4210909.2
Sum:	\$ 7708495	\$ 9635619	\$ 11562742
Total Data Loss Expenses:			
	\$ 10284919	\$ 12856153	\$ 15427383

Source: Tech//404 Data Loss Cost Calculator, www.tech-404.com.

Account Data Compromise Recovery (ADCR)

In October 2006, Visa implemented the ADCR program to help issuers reduce expense associated with managing the fraud that results from an account compromise event.

The ADCR program:

- Eliminates supporting documentation, filing fees and other associated fees
- Establishes a fixed time frame of up to 13 months for assuming liability for eligible fraudulent transactions
- Estimates the acquirer liability upon breach notification to better forecast financial impact of the data breach incident
- Calculates acquirer liabilities and issuer reimbursements based on estimates of losses in the aggregate

Source: Visa USA *Operating Regulations*, October 2009.

Payment Card Industry Data Security Standard

An Evolutionary Process

2000

PCI DSS originally began as five different programs by each payment network: Visa Card Information Security Program (CISP), MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program.

2001

Visa mandated CISP in 2001 to protect Visa cardholder data—wherever it resides—ensuring that members, merchants, and service providers maintained the highest information security standard. Simultaneously, mandates adopted by other payment networks.

2004

The Payment Card Industry Security Standards Council formed in December 2004, to align the individual network policies into the Payment Card Industry Data Security Standard (PCI DSS).

2006

September 2006, the PCI Security Standards Council (SSC) took over responsibility to own, maintain and distribute the PCI DSS and all its supporting documents. Visa Inc., however, continues to manage all data security compliance enforcement and validation initiatives for Visa data.

2009

PCI is probably the most technically comprehensive set of standards for insuring data security, but multiple other standards have evolved over the past decade:

- BS7799, ISF (ISO) Standards
- Basel II, Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley Act of 2002

Source: www.visa.com/usa, *Securing Payments Building Robust Global Commerce*, Visa International/Global Vision Group, 2005.

Payment Card Industry Data Security Standard

PCI 12 Requirements

Build and Maintain a Secure Network

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

Protect Cardholder Data

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

Maintain a Vulnerability Management Program

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

Implement Strong Access Control Measures

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

Regularly Monitor and Test Networks

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

Maintain an Information Security Policy

12. Maintain a policy that addresses information security

Source: PCI DSS

PCI DSS

Issues and Considerations

PCI DSS:

- Focuses on the technical aspects of insuring data security
- Provides a baseline for data security
- Takes an important step towards minimum standards for IT security
- Requires *Annual Compliance* that reflects the organization's data security at a point in time (much like a balance sheet) and must be adopted as an ongoing process
- Standards are way ahead of other industries (e.g., NACHA, HIPPA, education, government, social organizations, telecommunications, insurance)

Beyond PCI™

PCI DSS Certification

The PCI DSS certification process is primarily technical in nature and typically includes:

- Selection of a Qualified Security Assessor (QSA)
- Assessment of the 12 PCI DSS requirements to identify technical and related procedural gaps
- Audit results that are measured against technical best practices
- A remediation plan that addresses all identified gaps
- Validation that PCI DSS has been certified

Beyond PCI™

What is it?

GVGroup's "Beyond PCI™" employs a variety of tools to protect your business assets beyond the technical requirements of PCI DSS

Beyond PCI includes:

- Comprehensive assessment of business risk and impacts from a potential data security breach
- Solutions to mitigate risk and a cost/benefit prioritization of key resources and dependencies, including timing
- An on-going implementation and monitoring plan to manage identified risks
- Thorough response planning and execution when a data security breach occurs

Beyond PCI™

Audience

Beyond PCI targets entities that store, transmit or process customer data across the value chain of the payments industry

- Merchants and businesses
- Acquirer processors and third parties
- Banks/Financial institutions

Beyond PCI™

Modules

Beyond PCI is composed of three independent modules to better manage risk before and after a breach incident:

- 1. Identify and Assess**
- 2. Mitigate and Manage**
- 3. Respond and Control**

Beyond PCITM Modules

Module 1: Identify and Assess

Analyze, assess, document and quantify the impacts associated with a potential data security breach within each of the following areas:

- Brand, reputation, and market place positioning
- Multi-dimensional impacts on customers, e.g., sales, revenue, loyalty, competitive response
- Protection against liability, e.g., insurance, assurity/business continuity bonds
- State and federal legal and regulatory compliance
- Internal legal and regulatory compliance
- Payment network rules
- 3rd party/vendor underwriting and validation of PCI DSS compliance
- Merchant underwriting and validation of PCI compliance (processors, ISOs, acquirer banks)
- Staff training and on-going reporting
- Incident response planning and management

Beyond PCI™ Modules

Module 2. Mitigate and Manage

Design and manage the implementation of policies, procedures and programs to mitigate risk exposure to data breach incident

- Evaluate and prioritize gaps identified in Module 1
- Design and develop processes, procedures and programs to mitigate risk
- Enhance PCI to protect other business assets
 - Design and implement enhanced policies, procedures and standards
 - Improve risk mitigation programs of 3rd party vendors and support establishment of new relationships to reduce risk as appropriate
 - Implement detailed, ongoing reporting and assessments of vulnerabilities
 - Design and conduct staff training and awareness programs not covered under PCI
- Develop comprehensive remediation and response plan, including:
 - Data breach and forensic assessments
 - Legal, regulatory and payment network (PCI DSS) compliance
 - Customer and business impact assessment
 - Media and public relations campaign

“79 percent of U.S. consumer respondents cite loss of trust and confidence in any business they deal with as a consequence of a security or privacy breach.”⁺

⁺The CA 2008 Security and Privacy Survey, by CA Inc.

Beyond PCI™ Modules

Module 3. Respond and Control

Assist in quickly responding to and managing the impacts of a data breach incident

- Recognize that the organization has suffered a compromise
- Identify and recognize the source of the data breach
- Mobilize and empower internal/external breach response team
- Analyze and assess the breadth and severity of the breach incident
- Contact appropriate legal, regulatory and payment networks
- Implement communication responses and manage all aspects of plan
- Review and adjust plan in response to customer and business needs
- Respond to and prepare for legal and litigation issues
- Manage, review and adjust processes and procedures to avoid repeat incidents

Beyond PCI™ Checklist

GVGroup "BEYOND PCI"								
Addressed by PCI-DSS								
Technical Review and Certification					Protection of Other Business Assets			
PAYMENT BUSINESS	Technical PCI Gap Analysis	Technical 12 Requirements	Technical QSA Selection Process	Mitigate	Identify	Mitigate	Respond	
Merchant Business	✓	✓	✓	✓	technical only	no	no	
Acquirer / Processor	✓	✓	✓	✓	technical only	no	no	
Beyond PCI & Not Addressed by Payment Card Industry Standards								
Module 1: Identify and Assess								
Analyze, assess, document and quantify the impacts associated with a potential data security breach								
PAYMENT BUSINESS	Quantification of Brand, Reputation & Positioning Impacts	Multi-dimensional impacts on Customer Base	Liability Protection, e.g. insurance, bond, etc.	State and Federal Legal, Regulatory & Compliance Assessment	Internal Legal, Regulatory & Compliance Assessment	Payment Network Rules Review (non-technical)	3rd party/vendor underwriting and validation of PCI compliance	Merchant underwriting and validation of PCI compliance
Merchant Business	✓	✓	✓	✓	✓	✓	✓	
Acquirer / Processor	✓	✓	✓	✓	✓	✓	✓	✓
Module 2: Mitigate and Control								
Design and manage the implementation of policies, procedures and programs to mitigate risk exposure to data breach incident								
PAYMENT BUSINESS	Technical Component Risk Identification	Design & Develop Processes, Procedures for Mitigation Plan	Identify and assess risk mitigation programs of 3rd party vendors	Implementation of Policies, Procedures & Standards	Design and conduct staff training and awareness programs	Media/Public Relations Response Management	Develop comprehensive response plan	
Merchant Business	✓	✓		✓	✓	✓	✓	
Acquirer / Processor	✓	✓	✓	✓	✓	✓	✓	

For More Information About Beyond PCI

Contact:

Thomas A. Layman
President
Global Vision Group
147 17th Avenue, Suite A
San Mateo, CA 94402
650-349-1536
Email: tlayman@gvgroup.net