

# Privacy and Data Security Compliance

Jeff Carroll  
Terry Ramos  
Rachel Matteo-Boehm  
Eric Johnson



**WITS**

WINE INDUSTRY  
**TECHNOLOGY**  
SYMPOSIUM

July 15, 2008 - The Napa Valley Marriott

# Quick Shipping Compliance Update

- Illinois: New permit system as of June 1<sup>st</sup>
- Georgia: Dropped distributor prohibition as of July 1<sup>st</sup>
- Wisconsin: New permit system takes effect October 1<sup>st</sup>
- Ohio: Capacity cap increased to 250k gallons
- New York: Now requires electronic filing
- Massachusetts: FWC oral argument July 29<sup>th</sup>
- Tennessee: Potential challenge to federal onsite provision



# Age Verification

## Michigan

... obtain a copy of photo identification ... or utilize an identification verification service. You must record the name, address, date of birth and telephone number of the person placing the order on the order form.

## Georgia

- ...verify the age of such person placing the order either by the physical examination of an approved government issued form of identification or by utilizing an internet based age and identification service

## Ohio

- ...verify that the personal consumer is at least twenty-one years of age by checking the personal consumer's driver's or commercial driver's license or identification card.



# PCI Compliance

by Terry Ramos, VP Strategic Alliances Qualys



**WITS**  
WINE INDUSTRY  
**TECHNOLOGY**  
SYMPOSIUM

July 15, 2008 - The Napa Valley Marriott

# History of PCI Payment Card Industry

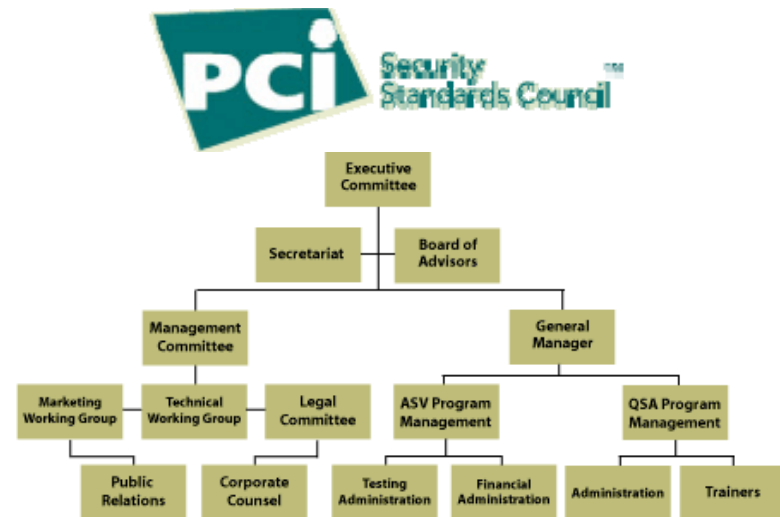
- Visa and MC have had their own Security Programs for years, with separate, and sometimes conflicting, requirements.
  - CISP & QDSC (VISA)
  - SDP (MC)
- Due to rampant Data Breaches & Credit Card Fraud, a unified approach was needed.
- The PCI Council was founded.



# PCI Security Standards Council

- New organization formed to promote PCI compliance and standards.

- Founded By:
  - American Express
  - Discover Financial Services
  - JCB
  - MasterCard Worldwide
  - Visa International



- Approves Certified Vendors
  - Approved Scanning Vendors (ASV) – Quarterly Scans
  - Qualified Security Assessor (QSA) – On-Site Audits



# PCI Data Security Standard

- The PCI Council published the PCI DSS –Data Security Standard
  - Outlined the minimum data security protection measures that needed to be in place to process, transmit or store credit card data.
  - Defined Merchant & Service Provider Levels, and validation requirements.
- In September 2006 the PCI Council updated the PCI DSS to v1.1 Adoption and/or enforcement dates varied between Credit Card Brands. As of 2007, all previous security programs have expired and merchants must follow PCI DSS v1.1



# Adoption of PCI

- PCI DSS published, promoted, email notifications, etc...
- Adoption of PCI has been driven through the use of incentives & fines
- Incentives have been offered to merchants and acquiring banks in the form of one-time payments and reduced interchange rates.
- Fines have been assessed to merchants who have failed to comply
- Acquirers submit plans on how they will support PCI for all merchants
















## PCI DSS is based on fundamental data security practices

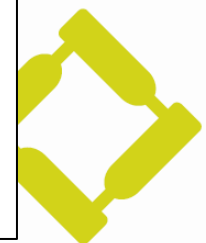
<b>Build and Maintain a Secure Network</b>	<ul style="list-style-type: none"> <li>• Install and maintain a firewall configuration to protect data</li> <li>• Do not use vendor-supplied defaults for system passwords and other security parameters</li> </ul>
<b>Protect Cardholder Data</b>	<ul style="list-style-type: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



# PCI Certification Merchant & Service Provider Levels

MERCHANT & SERVICE PROVIDER LEVELS & VALIDATION ACTIONS					
	LEVEL	CRITERIA	ON-SITE SECURITY AUDIT	SELF-ASSESSMENT QUESTIONNAIRE	NETWORK SCAN
MERCHANT	1	<ul style="list-style-type: none"> <li>- Any merchant, regardless of acceptance channel, processing <b>more than 6 million transactions</b> per year</li> <li>- Any merchant that suffered a security breach, resulting in an account compromise</li> </ul>	Required Annually *		Required Quarterly 
	2	- Any merchant processing between <b>150,000 to 6 million transactions</b> per year		Required Annually 	Required Quarterly 
	3	- Any merchant processing <b>between 20,000 to 150,000 transactions</b> per year		Required Annually 	Required Quarterly 
	4	- <b>All other merchants</b> not in Levels 1, 2, or 3, regardless of acceptance channel		Required Annually 	Required Quarterly 
SERVICE PROVIDER	1	- <b>All processors and all payment gateways</b>	Required Annually *		Required Quarterly 
	2	- Any service provider that is not in Level 1 and stores, processes or transmits <b>more than 1 million accounts / transactions</b> annually	Required Annually *		Required Quarterly 
	3	- Any service provider that is not in Level 1 and stores, processes or transmits <b>less than 1 million accounts / transactions</b> annually		Required Annually 	Required Quarterly 

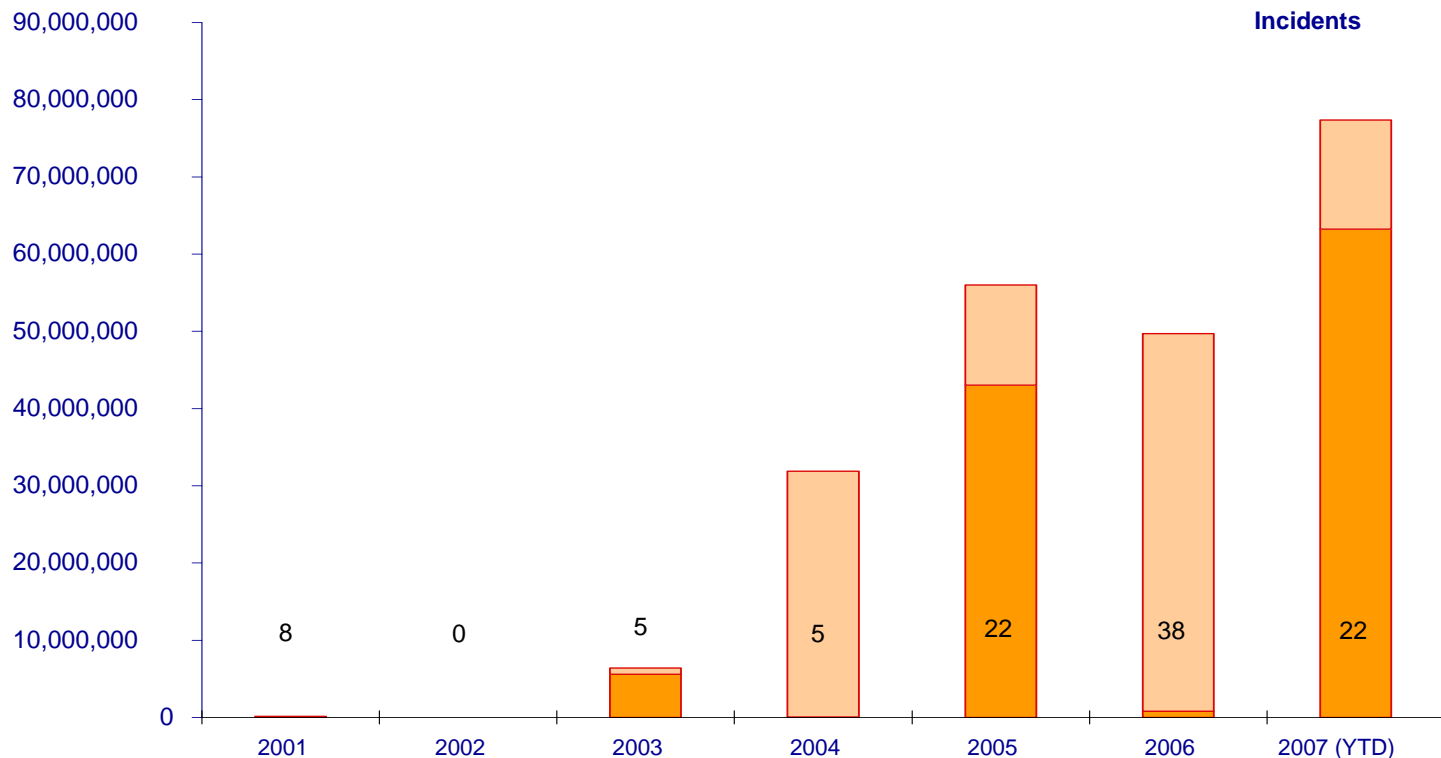
\* On-Site Security Audits may be conducted through Qualys PCI Consulting Partners - <http://www.qualys.com/partners/pci>



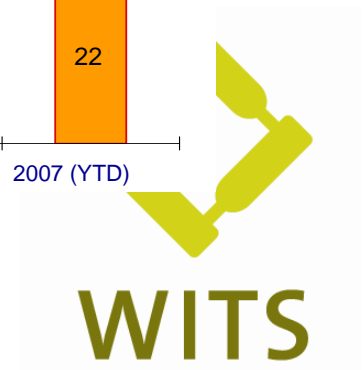
**WITS**

# Data Compromises are on the Rise

**A combination of increasing data breaches and state disclosure laws has resulted in a sharp rise in reported security compromises**



Source: [www.etiolated.org](http://www.etiolated.org) – includes all reported data compromises through August 2007



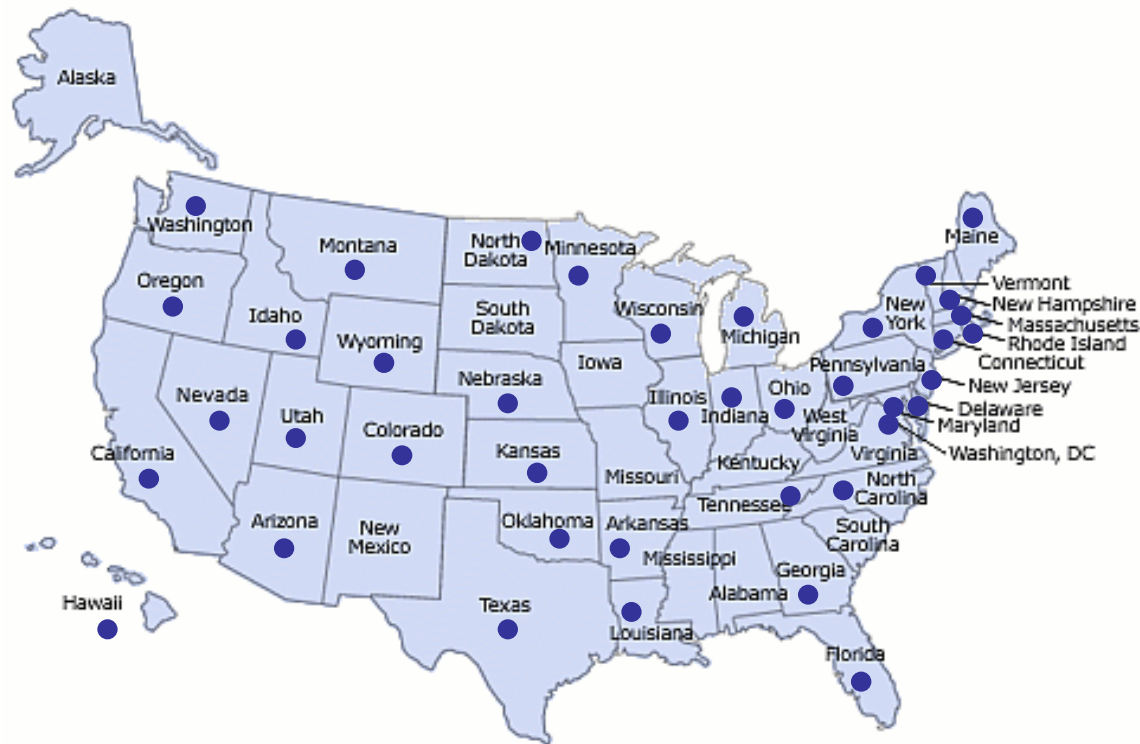
# Account Compromise - Impacts

- Counterfeit cards and fraud
- Significant chargeback risk
- Penalties, fines, losses
- Damage to reputation
- Negative media coverage
- Impacts to consumer confidence
- Re-issuance and monitoring of cards
- Potential of new legislation



# State Legislation

At least 40 states have enacted legislation requiring consumer disclosure of a security breach of personal information



Source: [http://www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf).



# Top 5 Vulnerabilities

**Based on merchant compromises, Visa has found the following common vulnerabilities:**



1. Storage of prohibited data (e.g., full track, CVV2, PIN blocks)
2. Vendor default accounts and passwords
3. Insecure remote access by software vendors
4. Compatibility issues with anti-virus and encryption
5. Poorly coded web-facing applications resulting in SQL injection

[www.visa.com/cisp](http://www.visa.com/cisp)



# Top 5 Reasons: Data Compromise

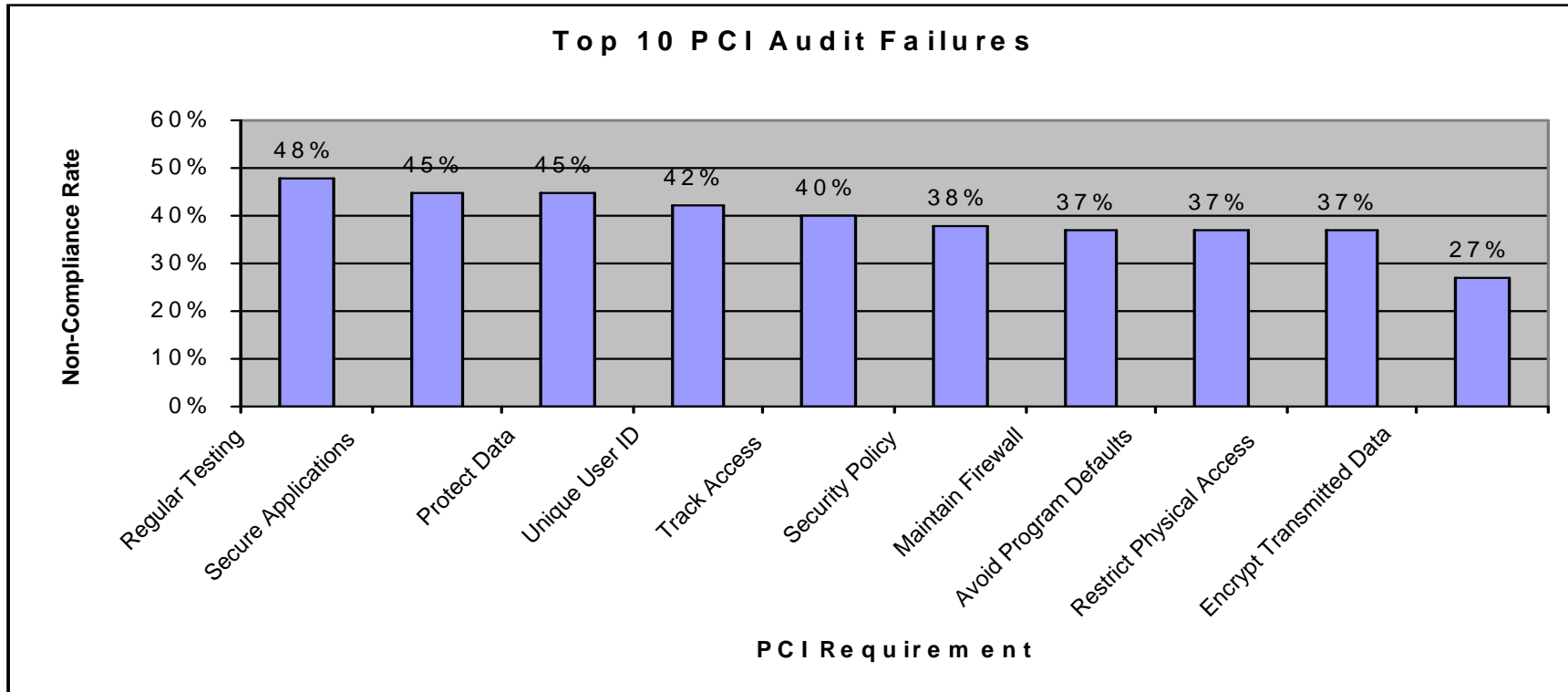
- 1 Ineffective Patch Mgmt
- 2 No Security Scanning
- 3 Weak Network Security
- 4 SQL Injections
- 5 Lack of Real Time Monitoring



Source: MasterCard Forensics Examinations of Hacked Entities



# Top 10 PCI Audit Failures



Based on a sampling of 60 assessments through July 17, 2007





# Shocking Trends



- Historically, no companies pass a PCI assessment on their first attempt
- Of the 60 sampled ROCs, 32 (or 53%) of the companies failed in some way (73% failed last year)
- Almost half (48%) of assessed companies did not comply with requirement #11

Source: VeriSign Professional Services



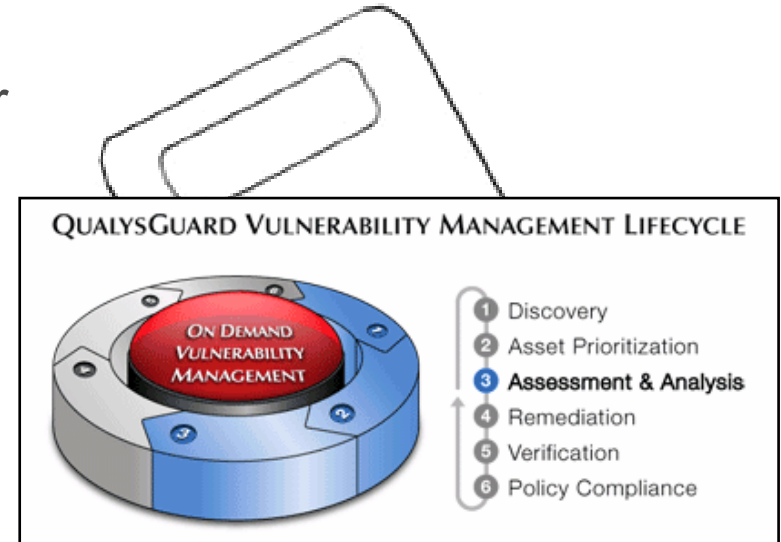
# Key to Security: Network Scanning

“... the countermeasure that will protect you, should a hacker scan your machines with a scanner is to **scan your own systems first.**”

Make sure to address any problems and then a scan by a hacker will give him no edge.”

Hacking Linux Exposed

Bottom Line: **Attacks target security vulnerabilities**



**WITS**

# What is Network Security Scanning ?

- **Find & Fix Weaknesses Proactively**

Security professionals run scans to find and fix vulnerabilities.

- **Hacker's Eye View**

Scanning takes an “outside-in” approach to security, emulating the attack route of a hacker.

- **Measurement of Security Posture**

Understand your security.



- **Act Fast or Risk Attack**

Hackers also scan systems to find potential vulnerabilities and exploit them using freely available tools.



# Network Scanning for PCI

- PCI Requires you run both Internal and External Network Vulnerability Scans at least Quarterly
- Internal Scans can be run by in house security staff
- External Scans must be performed by an Approved Scanning Vendor, and are then used to satisfy your Validation Requirements i.e. submit proof-of-compliance to your acquiring bank.
- By default, all externally facing IP addresses are 'in-scope'.
  - If proper segmentation exists the scope can be limited to just the IPs involved in credit card processing.



# Practical Tips for avoiding PCI Failure

- Store Less Data, and Encrypt!
  - You don't have to secure what you don't have.
- Understand your Data Flows
  - Is there anyone that knows your data flow end to end?
- Address App & Net Vulnerabilities
  - Do you know the real risk?
- Improve Security Awareness
  - People ARE the weakest link!
- Monitor Systems for Intrusions
  - Monitor to Stop and Prevent!
- Segment Credit Card Networks
  - Still the most effective way to reduce PCI Scope



# Store Less Data

- What do you NEED to store?
  - What data is available to you?
  - What are the business and legal needs?
  - Where do you need to store this?
  - What is the risk associated?
- Ask the hard questions!
  - Why do you need this?
  - What would you do without it?
- What to do with risk?
  - Accept it (and face fines!)
  - Mitigate it
  - Insure it

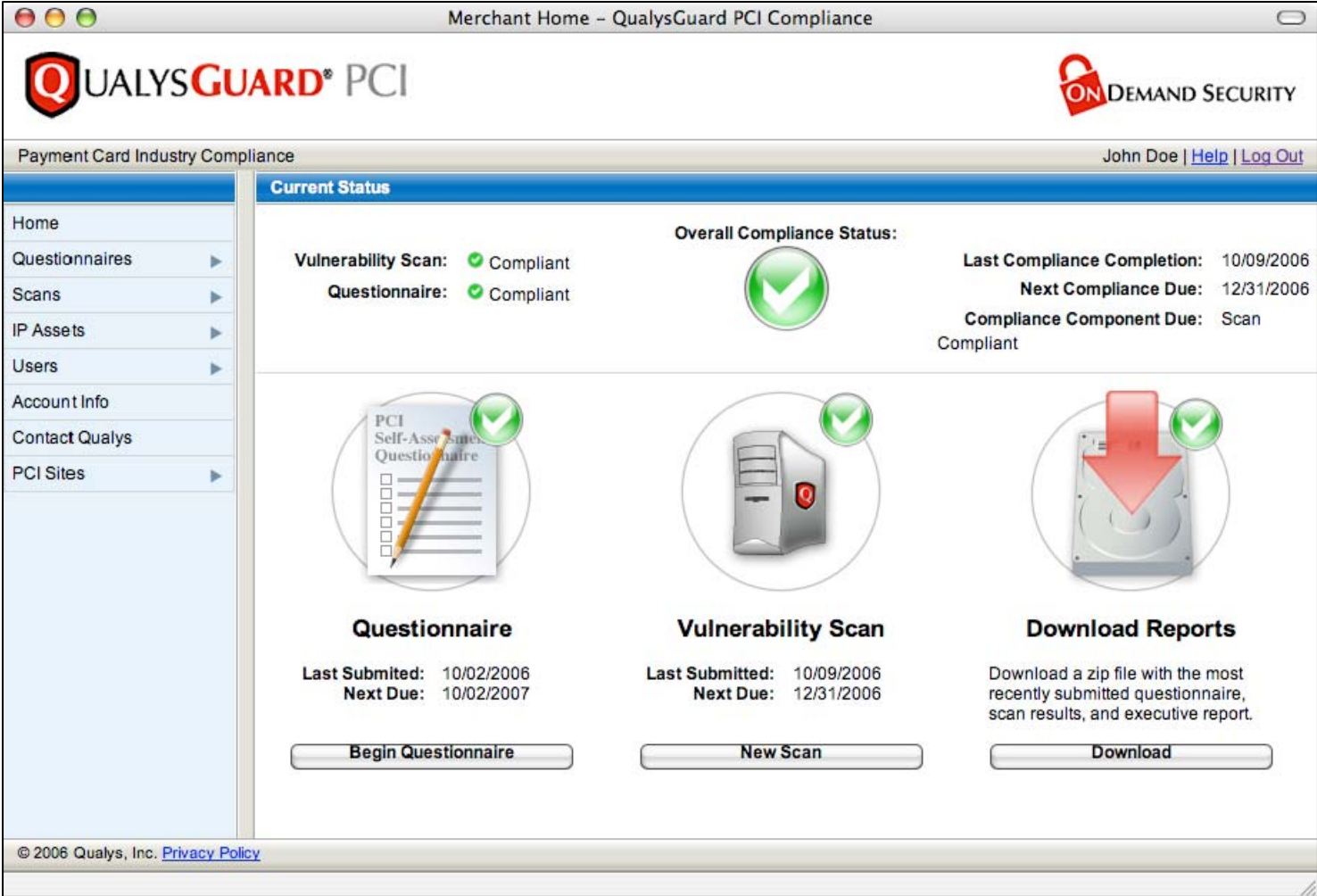


# Address Vulnerabilities

- Update POS Applications
  - Visa maintains a list of non-compliant POS applications, be sure you are running a compliant version
- Identify Poorly Coded Web Apps
  - Perform code review or application testing to ensure code is secure
- Perform Quarterly Scans (11.2)
  - And be sure to include applications
- Implement Strict SDLC Processes
  - Try tracking vulnerabilities by developer



# 3 Simple Steps to Validate PCI Compliance





# Steps to complying with PCI DSS

- Adhere to PCI DSS and perform Required Validation
- Appoint responsibility with Finance/Treasury
- Review & Document your card processing flows
- Create a PCI DSS program management team
- Complete PCI DSS audit & scan
- Remediate security issues identified during audit & scan
- Complete verification audit & scan
- Obtain Safe Harbour
- Manage ongoing PCI DSS compliance
- Build Incident Response Team



# Summary

- PCI is a standard that can be understood and followed.
- All major Credit Card companies are supporting the standard.
- Quarterly compliance is a requirement regardless of Merchant or Service Provider Level.
- It is important to choose the right solutions and vendors to help you secure your critical data and automate the compliance process.
- Additional Information can be found at:
  - <https://www.pcisecuritystandards.org/>
  - [http://www.qualys.com/pci\\_compliance/wesem/](http://www.qualys.com/pci_compliance/wesem/)



# Q&A

Free PCI Trial at:

[http://www.qualys.com/forms/trials/qg\\_pci/matrix/?lsid=6851](http://www.qualys.com/forms/trials/qg_pci/matrix/?lsid=6851)



# Thank You

[tramos@qualys.com](mailto:tramos@qualys.com)



# Wine Sales In An Information Age: Legal Risks On And Offline

Rachel Matteo-Boehm  
Holme Roberts & Owen LLP  
San Francisco, CA



**WITS**  
WINE INDUSTRY  
**TECHNOLOGY**  
SYMPOSIUM

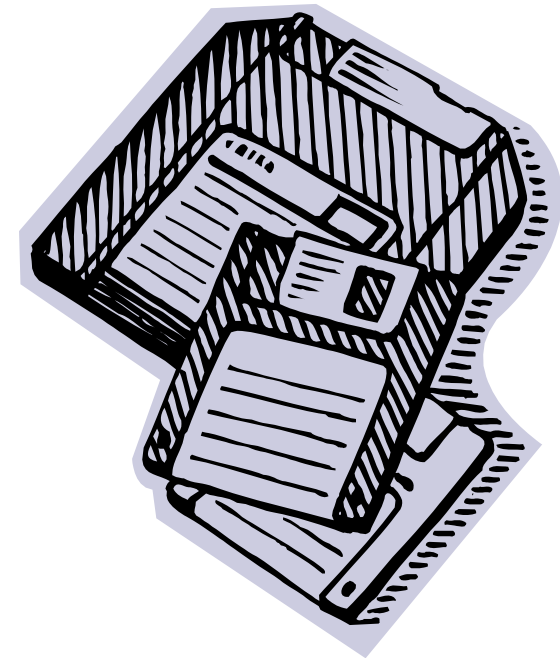


Holme Roberts & Owen LLP  
*Attorneys at Law*

“!”  
Experience Listens. Be Heard.™

July 15, 2008 - The Napa Valley Marriott

# Part One: Legal Consequences Of Data Breaches



# Data breach laws

- California was leader; security breach notification law was enacted in 2002 and became effective July 1, 2003.
- Since then, data breach notification laws have been enacted in more than 40 states
- Laws apply to both online **and** offline data
- Shifting legal landscape: new laws being enacted; existing laws being updated, possibility of federal legislation
- Penalties for noncompliance: civil and criminal penalties; private right of action for some laws; FTC action



# California security breach notification law: Cal. Civil Code § 1798.82

- Applies to “any person or business that conducts business in California”
- Breach = “Unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity” of personal information pertaining to a California resident



## Maintenance of personal information: Cal. Civil Code § 1798.81.5

- “A business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification or disclosure.”
- If personal information is maintained by a third party, business must “require by contract” observance with security practices/procedures





# California Law

- Notice-triggering personal information:
  - Unencrypted first name or initial and last name **plus** any of the following:
    1. Social security number
    2. Driver's license number or CA ID card number\*
    3. Financial account number, in combination with any required code or password permitting access to an individual's financial account
    4. Certain medical information
    5. Certain health insurance information



# California Law

- Timing of notice:
  - Must be given “in the most expedient time possible and without unreasonable delay” after discovery of breach
  - Cal. Office for Privacy Protection recommends that notice be given within 10 business days.
  - Limited delay OK if necessary to determine the scope of the breach and restore the security of the data and/or to avoid impeding a criminal investigation



# California Law

- Contents: as per Cal. Office of Privacy Protection, notice should include:
  - A general description of what happened
  - Identify particular personal information involved
  - What you have done to prevent further unauthorized acquisition
  - What your business will do to assist affected individuals, together with a toll-free number to call for further information and assistance and contact information for the CA Office of Privacy Protection
  - Information on what individuals can do to protect themselves from identity theft



# California Law

- Permissible methods for giving notice:
  1. Written notice
  2. E-mail, if you normally communicate with the individual by e-mail and have received their prior consent to that form of notification as per requirements of 15 U.S.C. § 7001
  3. Substitute notice, if (1) providing notice under first two methods would be more than \$250,000; (2) the affected class exceeds 500,000; or (3) the person or business does not have sufficient contact information. Methods of giving substitute notice include e-mail, posting on the business' web site, and notification to major statewide media



# Other state breach laws

- While many states' laws are modeled after the California law, other laws may differ several important respects, such as:
  - Nature of notice-triggering information
  - Application to paper as well as computer data
  - Number of individuals that must be affected before notice is required
  - Timing of notice; form and content of notice
  - Requirement to notify law enforcement or other government agencies
  - Civil or criminal penalties; in some states (like CA) affected individuals can sue for noncompliance

# If a breach happens to you ....

- Response must take into account all applicable state data breach laws
- Early detection of possible breach and prompt action upon learning of same is critical; allows time for investigation and the formulation of an appropriate response; in event a breach has occurred, acting quickly enables notification to affected persons within the time provided by law
- Handle with care (consult an attorney!)



# Data breach resources

- General information:
  - California Office of Privacy Protection:  
[www.oispp.ca.gov/consumer\\_privacy/default.asp](http://www.oispp.ca.gov/consumer_privacy/default.asp)
  - Federal Trade Commission:  
[www.ftc.gov/bcp/online/edcams/infosecurity/index.html](http://www.ftc.gov/bcp/online/edcams/infosecurity/index.html)
  - Privacy Rights Clearinghouse:  
[www.privacyrights.org/ar/ChronDataBreaches.html](http://www.privacyrights.org/ar/ChronDataBreaches.html)

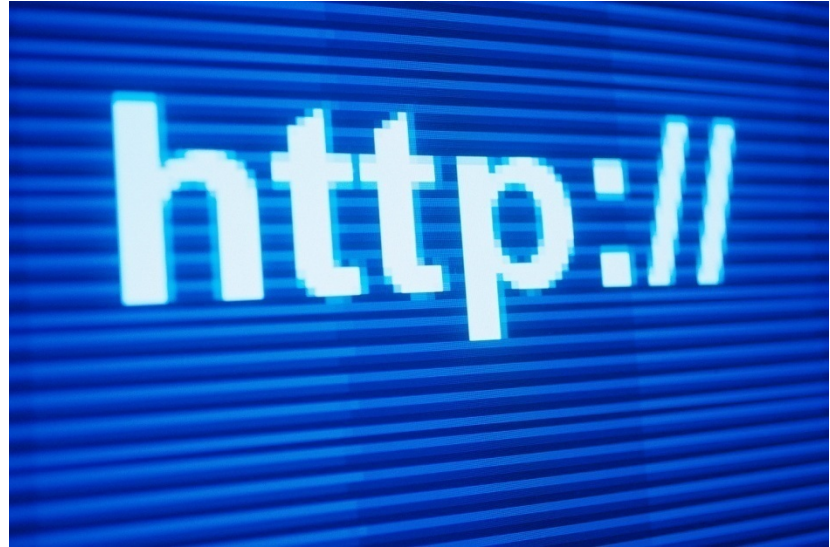


# Data breach resources

- State-by-state listings of breach laws:
  - Consumers Union:  
[http://www.consumersunion.org/campaigns/Breach\\_laws\\_May05.pdf](http://www.consumersunion.org/campaigns/Breach_laws_May05.pdf)
  - CSO:  
[http://www.csoonline.com/article/221322/CSO\\_Disclosure\\_Series\\_Data\\_Breach\\_Notification\\_Laws\\_State\\_By\\_State/1](http://www.csoonline.com/article/221322/CSO_Disclosure_Series_Data_Breach_Notification_Laws_State_By_State/1)
  - National Conference of State Legislatures:  
<http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm>



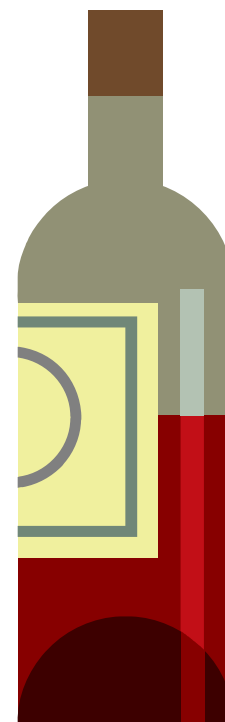




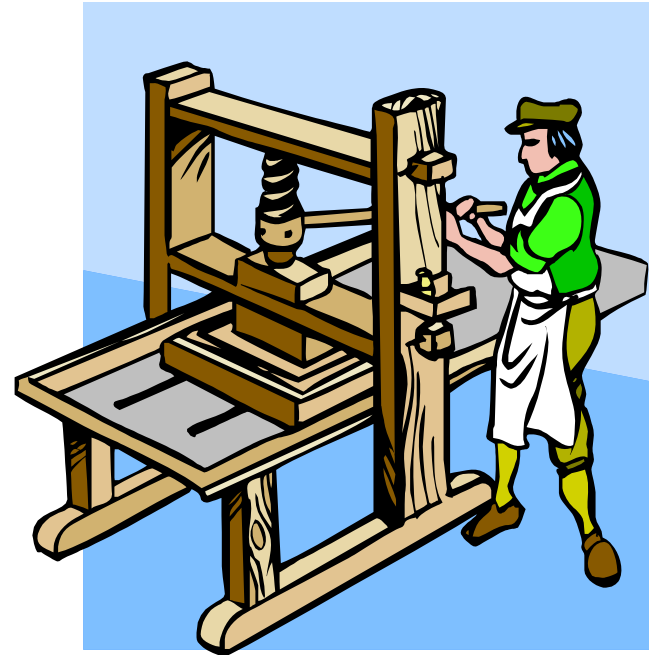
# Part Two: Internet 101



You may think you are in the wine business, but thanks to the Internet, you also are (or soon will be) in a second business . . .



# The publishing business!



# Web publishing risks

- Web publishers face many of the issues that have confronted traditional publishers (e.g., newspapers, magazines), along with some new issues and twists on the old ones
- Web publishing risks and requirements:
  - Liability for libel, trade libel, copyright infringement, trademark infringement, false advertising, misappropriation, and other content-related risks;
  - Privacy issues
  - Contractual issues



# Content risks: rules of the web

- **Rule #1**

You are on the hook for everything you or your agents post to your web site (text, photos, graphics, video, etc.), just like you would be in the paper-based world.

- **Rule #2**

In most cases, you are probably ***not*** on the hook for user-generated content (“UGC”), so long as you follow certain precautions and comply with certain legal requirements. This makes the web different than the paper-based world.



# Content risks: libel

- Libel =
  - Defamatory statement (anything that hurts the reputation of another person)
  - False statement of fact (vs. nonactionable opinion)
  - Statement is about the individual plaintiff (vs. a statement about a large group)
  - Statement is not privileged
  - Statement is made with the requisite degree of fault
  - Attribution is not a defense: in general, the fact that you attribute a statement to someone else does not eliminate your legal responsibility for repeating the statement, and is not a defense to a claim for libel

# Content risks: trade libel

- Trade libel is similar to regular libel, except that trade libel applies where the defamatory statement is made about the quality of a person's goods (e.g., wine, grapes) or services (e.g., bottling service, storage facility).
- In contrast, libel focuses on statements that damage the reputation of a **person**.



# Content risks: copyright infringement

- Protection for any “original work” that is “fixed in any tangible medium of expression.” Examples of copyrightable works: text, sound, pictures, graphics, symbols, photographs, video.
- No formalities required - A copyright owner need not register his work, nor is there any need to post any kind of notice to obtain copyright protection (labels such as “© 2008 Owner” are optional).
- Copyright owner - While copyright initially vests in the author of a work, an employer is, in most cases, the owner of works created by its employees.
- Penalties for infringement include money damages (up to \$150,000 for each work infringed for registered works); attorneys fees.



# Content risks: copyright infringement

- Contrary to popular belief:
  - Text, photographs, and other materials available on the Internet are **not** “public domain” works available for all to use.
  - Material on the Internet may be off limits even though it is not accompanied by a “©” or similar attribution, and even though you might not know the identity of the author.
  - Using material found on the Internet – whether on your own web site or in some other way – is not always “fair use”



# Other content risks

- Trademark infringement – Using someone else’s trademark or service mark in your web site without their consent or other justification, or using a trademark or service mark that is confusingly similar to someone else’s mark.
- Misappropriation/right of publicity – Use of another person’s name or “likeness” for commercial purposes (*i.e.*, on your web site) without their consent can make you liable to that person for violation of their “right of publicity,” even if they are not famous.
- False Advertising – False or misleading material on your web site can create liability under false advertising laws, even if it doesn’t seem like advertising per se. See *Kasky v. Nike*, 27 Cal. 4<sup>th</sup> 939 (2002).



# Special rules for UGC

- User generated content, or UGC = text, photos, video or other images posted by users of your web site (*i.e.*, someone other than you or your agents).
- Example: content posted by users to a blog or a forum.
- Website owner enjoys certain immunities from content-related claims, thanks to:
  - Section 230 of Communications Decency Act
  - Section 512 of Digital Millennium Copyright Act



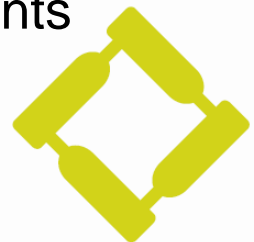
# Special rules for UGC

- 47 U.S.C. § 230 – Provides immunity from libel, misappropriation, false advertising, and other similar claims for providers and users of web sites that publish content generated by third parties. But:
  - No immunity for violation of federal intellectual property laws (e.g., copyright and trademark)
- Developing issue – How far can a web site operator go in editing and/or soliciting UGC without becoming the content provider? Beware of:
  - Adding titles/headings/short summaries
  - Adding content within text
  - Actively soliciting particular content
  - Using questionnaires to solicit particular content



# Special rules for UGC

- Section 512 of the Digital Millennium Copyright Act “DMCA” provides web site operators with immunity from copyright infringement claims stemming from UGC, but only if the web site operator:
    - Has no knowledge of infringing activity
    - Does not receive a direct financial benefit from the infringing activity
    - Has designed an agent to receive notification of any claimed infringement, registered that person with the U.S. Copyright Office, and provided notice to users
    - Has adopted and “reasonably implemented” a policy against repeat infringers
    - Complies with specified notice and takedown requirements
- 17 U.S.C. § 512(c) & (g).



# Privacy policies

- Cal. Business & Professions Code § 22575: requires the operator of a commercial web site that collects “personally identifiable information” through the web site about California residents must post a privacy policy on its web site that meets the requirements of § 22575.
- “Personally identifiable information” = name, address, email address, telephone number, social security number, or “any other identifier that permits the physical or online contacting of a specific individual.”



# Contents of privacy policy

- CA law – Policy must be “conspicuously posted” and (1) disclose what information is being collected and categories of persons and entities with whom the information is shared; (2) describe ways web site users can view/change their personal information; (3) describe how users will be notified of changes to policy; identify effective date of the policy
- FTC – Policy should comply with FTC fair information practice principles:  
<http://www.ftc.gov/reports/privacy3/fairinfo.shtm>

# Terms of service

- Why have terms of service? While privacy policies protect the users, terms of service typically protect the web operator, and include such things as disclaimers of warranties, limitation of liability, choice of forum.
- Enforceability - Like privacy policies, only way to ensure enforceability is to require users to signal their assent by clicking an “I agree” or other similar button.





# Thank you !

Rachel Matteo-Boehm  
Partner, Holme Roberts & Owen LLP  
[rachel.matteo-boehm@hro.com](mailto:rachel.matteo-boehm@hro.com)  
415-268-1996



Holme Roberts & Owen LLP  
*Attorneys at Law*

“!”  
Experience Listens. Be Heard.™



# PCI Compliance

Eric Johnson, Information Systems Project Manager



**WITS**  
WINE INDUSTRY  
**TECHNOLOGY**  
SYMPOSIUM

For Sales/Marketing/Direct-to-Consumer

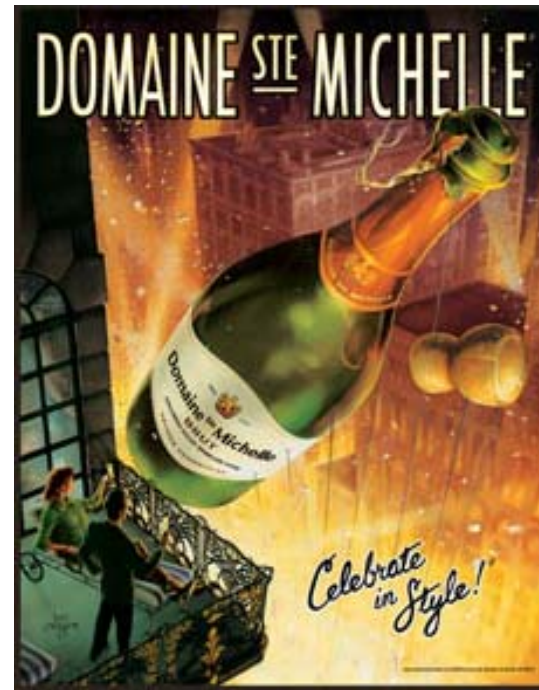
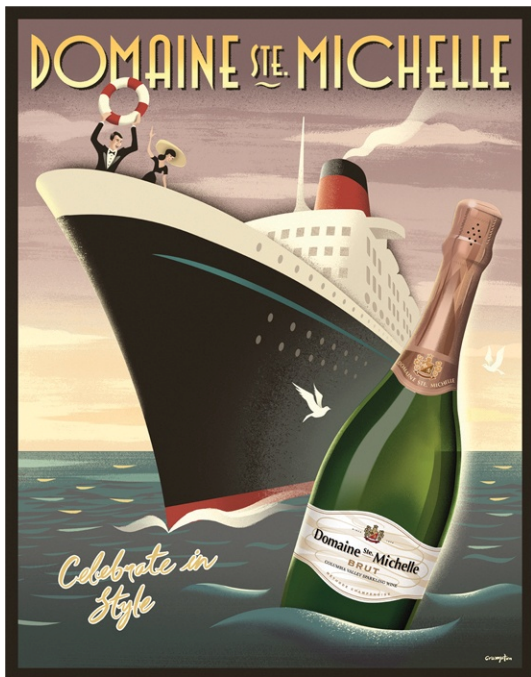
**Ste. Michelle Wine Estates**

[eric.johnson@ste-michelle.com](mailto:eric.johnson@ste-michelle.com)

July 15, 2008 - The Napa Valley Marriott

# Our history with PCI

- Small departmental project to sell posters – outsourced to a third party, who was compromised.



WITS

# Our history with PCI, cont.

- We alerted processor, became level 1
  - Normally reserved for largest merchants
  - On-site audits, perimeter scanning, etc.
  - Our entire wine operation was pulled into focus – multiple online stores, physical shops, clubs, etc.



# Lessons Learned

- ***Being*** PCI compliant is relatively easy if you follow good IS/IT security procedures.
  - Virus scanning, firewalls, don't use default passwords, encryption
  - Restrict info to need-to-know
  - Testing, business procedures, audit trails
- ***Proving*** your compliance is very expensive, especially at Level 1



# Lessons Learned, cont.

- You are responsible for your vendors' and employees' PCI compliance
- Software is only a piece of it
  - It can't, by itself, *make* you compliant, but it can *prevent* you from being compliant.
    - We had to entirely replace related systems – wine club, retail POS, etc.
  - Business and IT practices and procedures are the most important.
    - Paper is as big a risk as electronic data



Q & A

Questions?

