

Facing The Challenges of Merchant Compliance

Tanya Denysschen – Alliance Manager EMEA

April 15, 2008



Challenges with PCI DSS

Banks, Service Providers and Merchants alike face several challenges in the process of trying to drive compliance with PCI DSS

- Resource Constraints
 - ✓ No Budget
 - ✓ Lack of Expertise
- Merchant and Service Provider Identification
 - ✓ PCI Levels (1, 2, 3, 4)
 - ✓ High Risk Profiles
 - ✓ Validation Requirements
- Communication
 - ✓ Previous lack of information on PCI DSS
 - ✓ Inappropriate Tools for Internal and External Training

Current Statistics

Recent statistics show an increased willingness to validate compliance.

Europe

- Level 1 merchants
 - ✓ 10% Compliant
 - ✓ 33% In Progress
 - ✓ 30% Committed
 - ✓ 40% Preparing
- Level 2 and 3 merchants
 - ✓ 31% Compliant
 - ✓ 25% In Progress
 - ✓ 25% Preparing
- Service Providers
 - ✓ 350 Known Service Providers
 - ✓ 30% Compliant

U.S.A.

- Level 1 merchants
 - ✓ 44% of 325 level 1 compliant
 - ✓ 95% in progress
- Level 2 merchants
 - ✓ 25% compliant
- Service Providers
 - ✓ 250 known compliant

Compliance Programme Lifecycle

Generate awareness of PCI DSS among key stakeholders inside the business such as risk, compliance, financial and legal.

Determine your merchants risk or which merchants pose the greatest risk for loss.



Manage merchant through tools which validate compliance with PCI DSS in the quickest, most efficient manner possible.

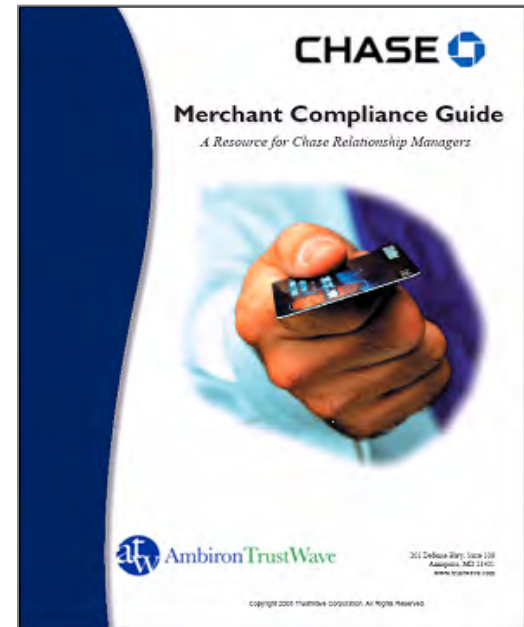
Convey compliance messages internally and to all affected merchants through a robust communication program to drive the message.

Education

Share information with key internal and external audiences

- Training for Key Audiences
 - ✓ Key Departments (IT, Compliance, Risk)
 - ✓ Sales / Relationship Managers
 - ✓ Customer Service Personnel
 - ✓ Executive Team

- Deliverables
 - ✓ PCI Awareness Seminars
 - ✓ Scoping meetings with QSA
 - ✓ Employee and Customer Facing FAQ
 - ✓ "Compliance Guides" (see right)



Materials are available to help educate on the PCI DSS compliance requirements

Risk Analysis

Automated risk analysis tools prioritise and categorise risk

- **Dynamic Questionnaire**
 - ✓ Brief - 8-12 questions
 - ✓ Intelligently populated
- **Risk Score**
 - ✓ High, Medium, Low
 - ✓ Action based on risk
- **Compliance Action Plan**
 - ✓ Client-size appropriate
 - ✓ Web-based compliance portal

Risk Profiler
Powered by TrustKeeper

AmbironTrustWave

Welcome to the Risk Profiler!

Welcome!

Protecting the cardholder data you process and/or transmit is critical to your business. AmbironTrustWave created the Risk Profiler to help you to first measure your risk, and then take the necessary steps to secure your customers' credit card information and comply with the Payment Card Industry (PCI) Data Security Standard.

The Risk Profiler registration and questionnaire takes only a few minutes to complete. You will provide some basic information about your business including contact information, credit card transaction volume and acceptance channels (i.e. e-commerce vs. brick and mortar). Once complete, you will receive instructions for the required next steps to become PCI compliant.

Enroll in the Risk Profiler today!

To enroll in the Risk Profiler, click the Start Risk Profiler button in the lower left portion of the page. If you received an enrollment code, please enter it in the box above the button. You would have received your enrollment code in a letter from your acquiring bank.

To obtain more information about AmbironTrustWave or our products and services, please click here to [e-mail](mailto:info@atwcorp.com) us or call us at 1-866-878-7817. Visit our website at www.atwcorp.com.

Are you at risk?

Find out in a minute or two with the TrustKeeper Risk Profiler.

If you have an Enrollment Code, enter it below:

START RISK PROFILER

Take the Next Step...

If you completed the Risk Profiler and are ready to take the next step toward TrustedCommerce, enter your information below to enroll. We will connect you to your Risk Profiler results.

Email

Account Number

Zip/Postal code

SUBMIT

Already Enrolled in TrustKeeper?

➤ **TrustKeeper Login**

Communication – Messaging and Promotion

Critical to inform your users about compliance issues

- Branding Exercise
 - ✓ Programme Name
 - ✓ Key Messages
 - ✓ Consistent Tone or “Voice”

- Co-Branded Deliverables
 - ✓ Corporate Website
 - ✓ Letter and Email Communication
 - ✓ Webinar Education Series
 - ✓ Statement Insert
 - ✓ Press Release
 - ✓ FAQ for Sales and Customer Service



Co-branded website marketing offers easy, hassle free enrollment to merchants

State-Of-The-Art Compliance Management

TrustKeeper® is a Web-based compliance validation solution

- Self assessment questionnaire verifies policies and procedures
- Vulnerability scanning engine identifies technology weaknesses
- Compliance report identifies non-compliance areas
- Remediation support provides compliance roadmap

The screenshot displays the TrustKeeper web application interface within a Microsoft Internet Explorer browser window. The address bar shows the URL: https://www.trustkeeper.net/esp/GoHome.action. The page header includes a welcome message for user 'sbakkenatw' and navigation links for Customer Support, Edit Profile, and Logout.

Overall Program Status: Compliant

Questionnaire Results: Pass
Last: Dec 7, 2006 2:46:13 PM CST
Expires: Dec 8, 2007

Vulnerability Scan: Pass
Last Scan: Nov 22, 2006 4:10:09 PM CST
Next Scan: Dec 22, 2006 4:00:00 PM CST

Compliance Program Roadmap:

- 1 Learn About The Program
- 2 Complete Questionnaires
- 3 View Results
- 4 Fix Problems

Card Association Security Standards & Programs:

- [Payment Card Standards Gap Analysis](#)
- [September 2006 changes within the PCI DSS requirements. This gap analysis details AmbionTrustWave's opinion as to the changes in the standard for our clients.](#)
- [Visa Cardholder Information Security Program](#)
- [Official site for information about Visa's](#)
- [Visa Account Information Security](#)
- [MasterCard Site Data Protection Program](#)
- [American Express Data Security Requirements](#)
- [Discover Data Security Guidelines](#)

Downloadable Security Guideline:

- [PCI Questionnaire](#)
- [Downloadable English version of PCI Qd](#)
- [PCI Questionnaire - Français](#)
- [Downloadable French version of PCI Qd](#)
- [PCI Data Security Standard](#)
- [This is the unified security standard endorsed by the major card associations.](#)

The interface also features a navigation menu on the left with options like Vulnerability Scan, Remediation, Questionnaires, and Security Resources. A 'Trusted Commerce Seal' is visible, along with a 'Payer Authentication' section. A smaller inset window shows a detailed security assessment table with columns for Risk, Name, and Recommendation.

Sponsor View - Adoption Campaign Example

■ Demand Generation:

- ✓ *Proactive Communication Strategy*
 - Targeted E-mails via Trustwave e-mail engine
 - Letters to select merchants
 - Statement communication
 - Webinars for select merchants

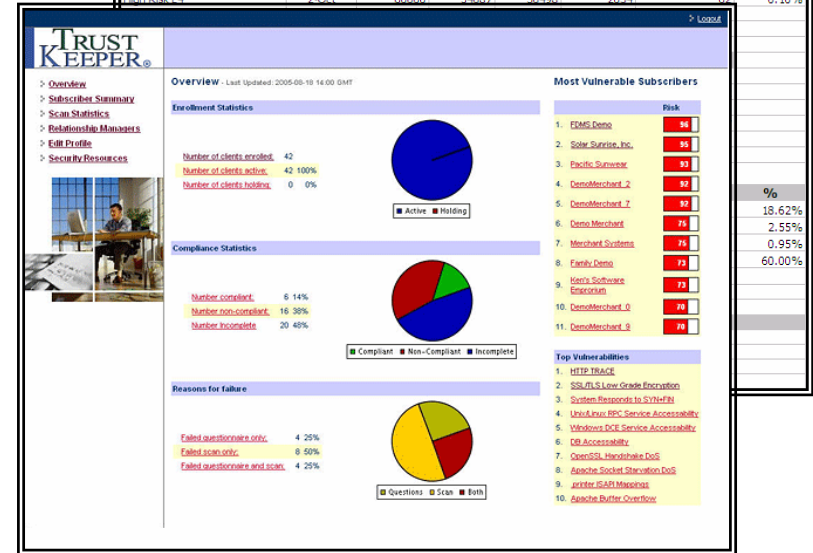
■ Reporting:

- ✓ *TKR Communication reports to identify:*
 - Compliant Merchants
 - Enrolled Merchants
 - "Listening" Merchants
 - "Un-interested" Merchants

■ On-Going Activity:

- ✓ *Campaign schedule*
- ✓ *Refresher internal education*
- ✓ *Milestone Communication (internal & external)*

Fifth Third Program Report							
Communications Reporting							
Activity	Date	Base	Target	Enrolled	% Target	% of Base	Converted
Letter Soft L4	29-Aug	1100	40	17	43%	1.55%	17
Conference Calls	14-Jun	20	10	15	150%	75.00%	15
Letter Top 2-3 merchants	14-Aug	2587	52	77	148%	2.98%	77
Letter High Risk L4	15-Sep	60000	600	60	10%	0.10%	60
Letter all L4	1-Oct	120000	1200	80	7%	0.07%	80
Total							249
Email Reporting							
Campaign	Date	Sent	Opened	Clicked	Resonded	Converted	%
Level 2-3	1-Aug	2500	1998	1400	10	25	1.00%
Higher Education Segment	2-Sep	150	142	135	25	89	59.33%
Restaurateur Segment	17-Sep	242	145	100	50	22	9.09%
High Risk L4	2-Oct	60000	54087	30498	2054	67	0.10%



TRUST KEEPER®

Overview - Last Updated: 2005-08-18 14:00 GMT

Enrollment Statistics

- Number of clients enrolled: 42
- Number of clients active: 42 100%
- Number of clients holding: 0 0%

Compliance Statistics

- Number compliant: 6 14%
- Number non-compliant: 16 38%
- Number incomplete: 20 48%

Reasons for failure

- Failed questionnaire only: 4 25%
- Failed scan only: 8 50%
- Failed questionnaire and scan: 4 25%

Most Vulnerable Subscribers

Rank	Subscriber	Risk	%
1	FMS Demo	94	18.62%
2	Solar Sunrise, Inc.	93	2.55%
3	Pacific Sunrise	93	0.95%
4	DemoMerchant_2	92	60.00%
5	DemoMerchant_7	92	
6	Demo Merchant	76	
7	Merchant Systems	76	
8	Family Demo	73	
9	Ken's Software Emporium	72	
10	DemoMerchant_0	70	
11	DemoMerchant_8	70	

Top Vulnerabilities

- HTTP TRACE
- SSL/TLS Low Grade Encryption
- System Responds to SYN/FIN
- Unix/Linux RPC Service Accessibility
- Windows SDC Service Accessibility
- DB Accessibility
- OpenSSL - Heartbleed DoS
- Apache Socket Starvation DoS
- Juniper SSM Missing
- Apache Buffer Overflow

Program Reporting is available through TrustKeeper and custom reporting documents

PCI DSS Key Messages



- Compliance is Mandatory
 - ✓ Learn how PCI affects you
 - ✓ Get started now
- Prepare
 - ✓ Risk analysis
 - ✓ Gap analysis
 - ✓ Self Assessment
- Plan Accordingly
 - ✓ Compliance takes time
 - ✓ Budget for remediation/audit
 - ✓ Annual procedure

Summary

Compliance is a good business practice

- Create a PCI Programme in your business
 - ✓ Education
 - ✓ Risk Analysis
 - ✓ Communication
 - ✓ Compliance Management
- Provides a clear path of action to address security risks
- Ensures your third party relationships do not put your business at risk
- Provides brand integrity and consumer confidence
- Protects against potential financial liabilities
- Compliance minimises the data security risk to your business

Thank You
Questions?