Guiding open standards for global payment card security

How You Can Participate

Why PCI?

How The Council Can Help You

How You Can Participate

Agenda
Your Card Data is a Gold Mine for Criminals

Types of Data on a Payment Card

- Chip
- Pan
- Expiration Date
- Cardholder Data
- Magnetic Strip (data on tracks 1 & 2)
- CAV2/CID/CVC2/CW2 (Discover, JCB, MasterCard, Visa)
- CID (American Express)
### They Steal Your Data … and They Sell It

<table>
<thead>
<tr>
<th>Bank and Location</th>
<th>Country</th>
<th>Balance</th>
<th>Price</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank of America (BOA)</td>
<td>USA</td>
<td>...</td>
<td>Sold</td>
</tr>
<tr>
<td>Amsouth Bank</td>
<td>USA</td>
<td>$16,040</td>
<td>€700</td>
</tr>
<tr>
<td>Washington Mutual Bank (WAMU)</td>
<td>USA</td>
<td>$14,400</td>
<td>€600</td>
</tr>
<tr>
<td>Washington Mutual Bank (WAMU)</td>
<td>USA, Multi-Currency Acct.</td>
<td>$7,950 + £2,612</td>
<td>€500</td>
</tr>
<tr>
<td>Washington Mutual Bank (WAMU)</td>
<td>USA</td>
<td>...</td>
<td>Sold</td>
</tr>
<tr>
<td>MBNA America Bank</td>
<td>USA</td>
<td>$22,003</td>
<td>€1,500</td>
</tr>
<tr>
<td>BANCO BRADESCO S.A.</td>
<td>Brazil, Dollar Account</td>
<td>$13,451</td>
<td>€650</td>
</tr>
<tr>
<td>CITIBANK</td>
<td>UK, GBP Account</td>
<td>£10,044</td>
<td>€850</td>
</tr>
<tr>
<td>NatWest</td>
<td>UK, GBP Account</td>
<td>£12,000</td>
<td>€1,000</td>
</tr>
<tr>
<td>BNP Paribas Bank</td>
<td>France, Euro Account</td>
<td>€30,792</td>
<td>€2,200</td>
</tr>
<tr>
<td>Caja de Ahorros de Galicia</td>
<td>Spain, Euro Account</td>
<td>€23,200</td>
<td>€1,200</td>
</tr>
<tr>
<td>Caja de Ahorros de Galicia</td>
<td>Spain, Euro Account</td>
<td>€7,846</td>
<td>€500</td>
</tr>
<tr>
<td>Banc Sabadell</td>
<td>Spain, Euro Account</td>
<td>€25,663</td>
<td>€1,450</td>
</tr>
</tbody>
</table>
Business Sectors With the Most Breaches

- Accommodation and Food Service 54%
- Retail Trade 20%
- Finance and Insurance 10%
- Healthcare and Social Assistance 4%
- Information 3%
- Other 6%

Source: Verizon 2012 Data Breach Investigations Report
Organizations Ignored PCI ... and Were Breached

96% of those breached were not PCI compliant as of their last assessment (or were never assessed/validated)

Top attack methods used to breach organizations:
- 81% of incidents involved hacking
- 69% incorporated malware
- 10% involved physical attack
### Top Mistakes By Those Breached

**Revealed by Forensic Audits**

<table>
<thead>
<tr>
<th>Mistake</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weak or Blank Password for an Administrative System Account</td>
<td></td>
</tr>
<tr>
<td>Sensitive Information Transmitted Unencrypted on the Wire</td>
<td></td>
</tr>
<tr>
<td>MS-SQL Server with Weak or No Credentials for Administrative Account</td>
<td></td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP) Cache Poisoning</td>
<td></td>
</tr>
<tr>
<td>Wireless Clients Probe for ESSID’s from Stored Profiles When Not Connected</td>
<td></td>
</tr>
<tr>
<td>Continued Use of Wired Equivalent Privacy (WEP) Encryption</td>
<td></td>
</tr>
<tr>
<td>Client Sends LAN Manager (LM) Response for NTLM Authentication</td>
<td></td>
</tr>
<tr>
<td>Misconfigured Firewall Rules Permit Access to Internal Resources</td>
<td></td>
</tr>
</tbody>
</table>

*Source: Trustwave 2012 Global Security Report*
EMV Environments Also Have Risks

+ Lost & Stolen Card Fraud now at its lowest level since the industry collation of fraud losses began in 1991

- EMV by itself does not protect the confidentiality of, or inappropriate access to sensitive authentication data and/or cardholder data
Compliance Is Good for Business

Cost of Complying

• Upgrading payment systems and security
• Verifying compliance via assessment
• Sustaining compliance
• May cost as little as $150 to $2,500 per IP address per year for scans for smaller merchants. Can cost millions for complex or older systems\(^1\)

Cost of a Breach

• Average cost per compromised record is $214
• Average cost of a breach event is $7.2 million
• Non-compliance cost is an average of 2.65 times the cost of compliance
• Also: business disruption, reduced productivity, fees, penalties, other legal and non-legal settlement costs\(^2\)

PCI Security Standards
Help You Protect Cardholder Data

Ecosystem of payment devices, applications, infrastructure and users

Guiding open standards for global payment card security
About the PCI Council

Open, global forum
Founded 2006

Guiding open standards for payment card security

- Develop
- Manage process
- Educate
- Foster Awareness
Global Representation, 600+ Members

- PayPal
- RSA, The Security Division of EMC
- Starbucks
- TSYS
- VeriFone Systems, Inc.
- Wal-Mart Stores, Inc.

- Barclaycard
- British Airways
- Cartes Bancaires
- European Payments Council
- IATA
- Ingenico
- Tesco Stores Limited

- Cisco
- Citi
- First Data Corporation
- Heartland Payment Systems
- JPMorgan Chase & Co.
- McDonald’s Corporation

- Cielo

* Board of Advisors

Guiding open standards for global payment card security
## The PCI Data Security Standard

<table>
<thead>
<tr>
<th>Six Goals</th>
<th>Twelve Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Build and Maintain a Secure Network</strong></td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td><strong>Protect Cardholder Data</strong></td>
<td>3. Protect stored cardholder data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td><strong>Maintain a Vulnerability Management Program</strong></td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td><strong>Implement Strong Access Control Measures</strong></td>
<td>7. Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td><strong>Regularly Monitor and Test Networks</strong></td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td><strong>Maintain an Information Security Policy</strong></td>
<td>12. Maintain a policy that addresses information security for employees and contractors</td>
</tr>
</tbody>
</table>

Guiding open standards for global payment card security
PCI Standards Help Secure Your Data

92% of compromises were simple

97% were avoidable through simple or intermediate controls

Source: Verizon 2012 Data Breach Investigations Report
You Drive the Open PCI Standards Lifecycle

Guiding open standards for global payment card security
## Your Feedback Shapes the Standards

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Feedback reviewed and categorized (April ‘12 – August ‘12)</td>
</tr>
<tr>
<td>2</td>
<td>Feedback shared with PCI community (August – September ’12)</td>
</tr>
<tr>
<td>3</td>
<td>Feedback presented at 2012 Community Meetings (September ‘12 – October ’12)</td>
</tr>
<tr>
<td>4</td>
<td>Revisions drafted for PCI DSS and PA-DSS (November ’12 – April ’13)</td>
</tr>
<tr>
<td>5</td>
<td>Final Review Period (May ’13 – July ’13)</td>
</tr>
<tr>
<td>6</td>
<td>Standards Published (October ’13)</td>
</tr>
</tbody>
</table>
PCI Security is a Journey...

...but reaching the summit holds immense value for your organization

96% of breach victims that are subject to PCI DSS had not achieved compliance

Source: Verizon 2012 Data Breach Investigations Report

Guiding open standards for global payment card security
Use the Standards to Make Security Part of Your DNA

- Reduce the attack surface
- Continuous Awareness & Protection
- Prevent New Types of Exposure
- Measure success and identify opportunity

Guiding open standards for global payment card security
Focused Guidance on Payment Technology

Mobile

P2PE

Virtualization

Wireless

Tokenization

Telephone-based Payment Card Data

EMV

Guiding open standards for global payment card security
Even EMV Security Needs PCI

- Council released guidance on EMV within an overall data security framework defined by the PCI Data Security Standard
- Guidance highlights benefits both systems bring to tackling fraud
- EMV does help prevent some types of fraud, but for a merchant to secure payment data they must also adopt all elements of the PCI DSS
- In today’s EMV market, PCI DSS must be fully implemented to protect cardholder data
**Point-to-Point Encryption**

**2012 Target Deliverables**

**General Requirements**
- P2PE Hardware encryption and hardware decryption
- P2PE “Hybrid” Hardware encryption and hardware decryption, with transaction keys in software at decryption
- P2PE next phase

**Point-to-Point Encryption**
- P2PE Assessor Qualification Requirements released
- Testing Procedures, Program Guide, SAQ and P2PE Assessor training now available
- Solutions listing for Fall 2012

*Sign up for P2PE Training today: administration@pcisecuritystandards.org.*
Mobile Update

Deliverable
Guidance and Best Practices
- Mobile Transactions Using SCR & P2PE for Merchants
- Mobile Acceptance Best Practices

Mobile
- Key areas of focus include:
  - Devices
  - Applications
  - Service Providers

Guiding open standards for global payment card security
Accepting Mobile Payment Acceptance Security Fact Sheet for Merchants

- Understand PCI DSS responsibilities in mobile environments
- Leverage benefits of P2PE program
- Choose a mobile payment acceptance solution that complements the merchant’s PCI DSS responsibilities
2012 Training Highlights

✓ Qualified Integrators and Resellers (QIR) Program
✓ Corporate PCI Awareness – Let Us Come To You!
✓ Online Awareness Training in Four Hours

To learn more, visit:
https://www.pcisecuritystandards.org/training/index.php
Make 2012 the Year of Data Security Training

PCI SSC Internal Security Assessor (ISA) Program
Helps security professionals improve their organizations’ understanding of PCI DSS and validate and maintain ongoing compliance

PCI Awareness Training
Offers general PCI training across your business to ensure a universal understanding of PCI compliance

2012 Training Schedule

**ISA Training:** Boston, MA, USA 20–21 August
**QSA Training:** Boston, MA, USA on 22-23 August
**ISA Training:** Lake Buena Vista, FL, USA on 6 – 7 September
**PA-QSA Training:** Lake Buena Vista, FL, USA on 8 – 9 September
**QSA Training:** Lake Buena Vista, FL, USA on 10 – 11 September
**ISA Training:** Lake Buena Vista, FL, USA on 10 – 11 September
**P2PE Training:** Lake Buena Vista, FL, USA on 15 – 16 September

Check out our Training Webinar!
What is the Qualified Integrators and Resellers (QIR) Program? PCI SSC certification program to educate, qualify, and train organizations involved in the implementation, configuration, and/or support of a PA-DSS validated payment application on behalf of a merchant.

Who can participate? Any eligible company involved in implementing and configuring PA-DSS validated applications into merchant environments, including both brick-and-mortar and e-commerce environments.

What are the benefits?

- Achieve industry-recognized certification
- Be included on merchants’ go-to global list of certified integrators and reseller
- Receive specialized training from PCI SSC experts on guidelines for implementing and maintaining payment applications
- Earn CPE credits

Online training will begin in fall 2012.

For more details, visit [www.pcisecuritystandards.org/training/qir_training.php](http://www.pcisecuritystandards.org/training/qir_training.php).

Please contact [QIR@pcisecuritystandards.org](mailto:QIR@pcisecuritystandards.org) with any questions.
Be Involved – Contribute Your Expertise!

Join! Become a Participating Organization today

Guiding open standards for global payment card security
Special Interest Groups (SIGs) Are For You

Risk Assessment  eCommerce  Cloud

sigs@pcisecuritystandards.org

Email today to join!

Guiding open standards for global payment card security
2013 SIG Proposal & Election Timeline

June 1, 2012
Proposal Period Open

July 31, 2012
Proposal Period Close

The Special Interest Groups (SIGs) leverage the valuable business and technical experiences of PCI SSC Participating Organizations to collaborate with the Council on any supporting guidance or special projects relating to the PCI Security Standards.

Submit your 2013 SIG proposal today!

• After the close of the SIG proposal period a shortlist of proposals will be drawn up by PCI SSC and those selected notified.
• Presentations from POs and assessors on shortlisted SIG proposals will be given at the North American and European Community Meetings.
• Electronic vote on which proposals to move ahead with will follow in November.

NEW for 2013: Online Proposal Form now available at https://www.pcisecuritystandards.org/site/sig-2012.php

Guiding open standards for global payment card security
2012 PCI Community Meetings

Orlando, Florida, USA
September 12-14, 2012

Dublin, Ireland
October 22-24, 2012

Register today:
http://www.regonline.com/pcissc_cm_orlando2012
http://www.regonline.com/pcissc_cm_dublin2012

Guiding open standards for global payment card security
Summary

**Learn!**
Take advantage of the Council’s resources and guidance, and training courses

**Join!**
Become a Participating Organization today

**Share!**
We want your feedback on the Standards

**Participate!**
Get involved in a Special Interest Group

Guiding open standards for global payment card security
Questions?

Please visit our website at  www.pcisecuritystandards.org