Protecting Cardholder Data

Best in Class Performance in Addressing
the PCI Data Security Standard

June 2007
Executive Summary

This research report provides new insights regarding the degree to which the 12 high-level security requirements of the Payment Card Industry (PCI) Data Security Standard (DSS) have been implemented, and the motivations and obstacles to implementation over the past 12 months. It also speaks to current and planned use over the next 12 months of key enabling technologies and services to aid in the achievement of PCI DSS compliance, and the benefits that Best in Class companies have derived from successful PCI DSS compliance initiatives.

Best in Class Performance

Based on feedback from more than 125 organizations, Aberdeen used the following key performance criteria to distinguish Best in Class companies in the protection of cardholder data from Industry Average and Laggard organizations:

- Have reported PCI compliance as a result of an internal audit or an external audit by a Qualified Security Assessor. 100% of Best in Class organizations have already reported PCI compliance.
- Have achieved higher levels of performance relative to their peers in the 6 high-level control objectives and 12 high-level security requirements of the PCI Data Security Standard, both currently and one year ago. Across all 12 security requirements, 86% of Best in Class organizations were rated at the highest levels of current performance, compared to 67% of the Industry Average.
- Have not experienced any breach, loss or disclosure of cardholder data in the last 12 months. 84% of Best in Class companies indicated that they had not experienced any breach, loss or disclosure.

Competitive Maturity Assessment

Survey results show that the companies enjoying Best in Class performance had several characteristics in common:

- 100% have built and maintained a secure network
- 95% protect cardholder data during storage, processing and transmission
- 68% have established and maintain a vulnerability management program
- 100% have implemented strong access control mechanisms
- 95% regularly monitor and test their networks
- 95% have established and maintain an information security policy
Required Actions

In addition to the specific recommendations in Chapter 3 of this report, to achieve Best in Class performance in the protection of cardholder data, organizations should:

- Take the strategic view that PCI DSS represents not only the best available framework to guide better protection of cardholder data, but also an opportunity to leverage cardholder data security achieved through PCI DSS compliance to drive better protection of other sensitive business data, and to address compliance with other standards and regulations.

- Ensure that strategy is properly aligned with execution. Once a clear strategic commitment to achieving PCI DSS compliance has been made, establish clear cross-functional ownership and adequate resource allocation for your organization’s compliance initiative.

“Looking back, I can’t think of a single case where we’ve said ‘that’s just not a reasonable requirement.’ In fact, we think some of them can still be tightened up a bit.”

~ Chief Technology Officer
Payment Processor
Table of Contents

Executive Summary.......................................................................................................2
  Best in Class Performance .........................................................................................2
  Competitive Maturity Assessment ..............................................................................2
  Required Actions .......................................................................................................3
Chapter One: Benchmarking the Best in Class..............................................................5
  The Payment Card Industry Data Security Standard .................................................5
  Maturity Class Framework .........................................................................................7
  Best in Class PACE Model ........................................................................................9
Chapter Two: Benchmarking Requirements for Success ..............................................11
  Competitive Assessment ..........................................................................................11
  Organizational Capabilities and Technology Enablers ............................................13
Chapter Three: Required Actions ...............................................................................15
  Laggards Steps to Success ......................................................................................15
  Industry Norm Steps to Success .............................................................................15
  Best in Class Steps to Success ................................................................................15
Appendix A: Research Methodology .........................................................................17
Appendix B: Related Aberdeen Research ....................................................................20

Figures

Figure 1: Leading Drivers for the Protection of Cardholder Data ...............................5
Figure 2: Current Performance in Meeting the 12 High-Level PCI DSS Requirements .................................................................................................................8
Figure 3: Leading Strategies for Protecting Cardholder Data .....................................10
Figure 4: Primary Responsibility for Your PCI Compliance Initiative ....................13

Tables

Table 1: Companies with Top Performance Earn “Best in Class” Status...............7
Table 2: Best in Class PACE Framework for Protecting Cardholder Data .........9
Table 3: Competitive Framework ..............................................................................12
Table 4: PACE Framework .......................................................................................18
Table 5: Maturity Class Framework ..........................................................................18
Table 6: Relationship between PACE and Competitive Framework 19
Chapter One: Benchmarking the Best in Class

The Payment Card Industry Data Security Standard

Public disclosures of security breaches involving consumer cardholder data are occurring with alarming frequency, some with stunning magnitude. In a well-known recent example (January 2007), some 45.7 million credit and debit card account numbers – plus 455,000 merchandise return records containing customer names and driver’s license numbers – were affected by an “unauthorized intrusion” into the computer systems of TJX, a leading off-price retailer of apparel and home fashions. This highly publicized disclosure came fully two years after American Express, Discover, JCB, MasterCard Worldwide and Visa International first announced a set of jointly developed worldwide data security standards for the payment card industry, and illustrates that companies within the payment card industry are at varying degrees of compliance with these industry best practices for protecting cardholder data.

Figure 1: Leading Drivers for the Protection of Cardholder Data

Source: Aberdeen Group, June 2007
To provide better protection for consumer cardholder data, the world’s leading payment card brands collaborated to develop a common Payment Card Industry (PCI) Data Security Standard (DSS), a unified worldwide standard for best security practices first announced in January 2005. The organizations that make up the global payment card industry – including merchants, banks, payment processors and service providers – are called upon to implement the policies, business processes, and a variety of enabling technologies necessary to help them achieve the following 6 high-level control objectives defined by the PCI DSS:

- Build and maintain secure networks;
- Protect cardholder data;
- Maintain a vulnerability management program;
- Implement strong access control measures;
- Regularly monitor and test networks; and
- Maintain an information security policy.

At the next level of detail, the PCI DSS uses these control objectives to define the following 12 high-level security requirements:

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

**Objectives for this Report**

This research report on protecting cardholder data and the PCI Data Security Standard was designed to give new insights into the following:

- The degree to which the 12 high-level security requirements of the PCI Data Security Standard have been implemented, and the motivations and obstacles to implementation over the past 12 months;
- The structure and effectiveness of existing PCI DSS implementations;
• Current and planned use over the next 12 months of key enabling technologies to aid in the achievement of PCI DSS compliance; and
• The benefits, if any, that have been derived from PCI DSS compliance initiatives.

For additional details on our research methodology, see Appendix A.

**Maturity Class Framework**

Aberdeen used the following key performance criteria to distinguish Best in Class companies in the protection of cardholder data from Industry Average and Laggard organizations:

• Have reported PCI compliance as a result of an internal audit or an external audit by a Qualified Security Assessor
• Have achieved higher levels of performance relative to their peers in the 6 high-level control objectives and 12 high-level security requirements of the PCI Data Security Standard, both currently and one year ago
• Have not experienced any breach, loss or disclosure of cardholder data in the last 12 months

Companies with top performance in the protection of cardholder data based on these criteria earn “Best in Class” status, as described in Table 1. (For additional details, see Table 5 in Appendix A.)

**Table 1: Companies with Top Performance Earn “Best in Class” Status**

<table>
<thead>
<tr>
<th>Maturity Class</th>
<th>Mean Class Performance</th>
</tr>
</thead>
</table>
| **Best in Class:** Top 20% of aggregate performance scorers | • 100% have reported PCI Compliance as a result of an internal audit or an external audit by a Qualified Security Assessor  
  • 86% have achieved a high level of current performance across the 12 high-level security requirements of the PCI DSS (for detailed breakdown, see Figure 2)  
  • 84% responded that they have not experienced any breach, loss or disclosure of cardholder data in the last 12 months |
| **Industry Average:** Middle 50% of aggregate performance scorers | • 48% have **not** reported PCI Compliance as a result of an internal audit or an external audit by a Qualified Security Assessor  
  • 67% have achieved a high level of current performance across the 12 high-level security requirements of the PCI DSS (for detailed breakdown, see Figure 2)  
  • 78% responded that they have not experienced any breach, loss or disclosure of cardholder data in the last 12 months |
| **Laggards:** Bottom 30% of aggregate performance scorers | • 73% have **not** reported PCI Compliance as a result of an internal audit or an external audit by a Qualified Security Assessor  
  • 21% have achieved a high level of current performance across the 12 high-level security requirements of the PCI DSS (for detailed breakdown, see Figure 2)  
  • 78% responded that they have not experienced any breach, loss or disclosure of cardholder data in the last 12 months |

Source: Aberdeen Group, June 2007
Figure 2: Current Performance in Meeting the 12 High-Level PCI DSS Requirements

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Industry Average</th>
<th>Best in Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintain a policy that addresses information security</td>
<td>69%</td>
<td>84%</td>
</tr>
<tr>
<td>Regularly test security systems and processes</td>
<td>44%</td>
<td>58%</td>
</tr>
<tr>
<td>Track and monitor all access to network resources and data</td>
<td>55%</td>
<td>58%</td>
</tr>
<tr>
<td>Restrict physical access to cardholder data</td>
<td>72%</td>
<td>90%</td>
</tr>
<tr>
<td>Assign a unique ID to each person with computer access</td>
<td>80%</td>
<td>95%</td>
</tr>
<tr>
<td>Restrict access to cardholder data by business need-to-know</td>
<td>68%</td>
<td>79%</td>
</tr>
<tr>
<td>Develop and maintain secure systems and applications</td>
<td>67%</td>
<td>100%</td>
</tr>
<tr>
<td>Use and regularly update anti-virus software</td>
<td>84%</td>
<td>100%</td>
</tr>
<tr>
<td>Encrypt transmission of cardholder data across open, public networks</td>
<td>66%</td>
<td>100%</td>
</tr>
<tr>
<td>Protect stored cardholder data</td>
<td>66%</td>
<td>95%</td>
</tr>
<tr>
<td>Do not use vendor-supplied defaults for system passwords and other security parameters</td>
<td>69%</td>
<td>79%</td>
</tr>
<tr>
<td>Install and maintain a firewall configuration to protect cardholder data</td>
<td>68%</td>
<td>94%</td>
</tr>
</tbody>
</table>

% of Respondents with Performance Rating = 4 or 5 (1=lowest, 5=highest)

Source: Aberdeen Group, June 2007
Best in Class PACE Model

Achieving superior protection of cardholder data requires a combination of strategic actions, business process capabilities and enabling technologies, as summarized in Table 2. (For a detailed description of Aberdeen’s PACE Framework, see Table 4 in Appendix A.)

Table 2: Best in Class PACE Framework for Protecting Cardholder Data

<table>
<thead>
<tr>
<th>Pressures</th>
<th>Actions</th>
<th>Capabilities</th>
<th>Enablers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect the organization and its brand from the negative consequences of potential highly publicized data breach disclosures</td>
<td>Use the Payment Card Industry (PCI) Data Security Standard (DSS) as the best available framework to guide implementation</td>
<td>Secure network</td>
<td>Firewalls</td>
</tr>
<tr>
<td></td>
<td>Leverage cardholder data security achieved through PCI DSS compliance to drive better protection of other sensitive business data, and to address compliance with other standards and regulations</td>
<td>Protection of cardholder data during storage and transmission</td>
<td>Configuration management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vulnerability management program</td>
<td>Data encryption for &quot;data at rest&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strong access control measures</td>
<td>Secure data transmission for &quot;data in motion&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Network monitoring and testing</td>
<td>Key management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information security policy</td>
<td>Anti-virus software</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure application development tools</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application firewalls / gateways</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Application vulnerability scanners</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Logical access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Two-factor user authentication</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Priviliged password management</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Physical access control</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Network / data monitoring, auditing and reporting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Aggregated log analysis, auditing and reporting (including SIM, SIEM)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Formal test plans for systems and processes</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Penetration testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Approved Scanning Vendors (ASV)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Qualified Security Assessors (QSA)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Formal risk assessment</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Formal information security policy</td>
</tr>
</tbody>
</table>

Source: Aberdeen Group, June 2007

In response to the pressure to protect the organization and its brand from the negative consequences of potential highly publicized data breach...
disclosures, 68% of Best in Class companies use the PCI Data Security Standard as the best available framework to guide their implementation for protecting cardholder data. In addition, Best in Class companies are 1.5X more likely than their Industry Average counterparts to use PCI DSS compliance as a springboard to address compliance with other standards and regulations. See Figure 3.

**Figure 3: Leading Strategies for Protecting Cardholder Data**

<table>
<thead>
<tr>
<th>Use the Payment Card Industry (PCI) Data Security Standard (DSS) as the best available framework to guide our implementation</th>
<th>Leverage cardholder data security achieved through PCI DSS compliance to drive better protection of other sensitive business data, and to address compliance with other standards and regulations</th>
</tr>
</thead>
<tbody>
<tr>
<td>68%</td>
<td>47%</td>
</tr>
<tr>
<td>50%</td>
<td>32%</td>
</tr>
</tbody>
</table>

Source: Aberdeen Group, June 2007

Aberdeen’s research shows that Best in Class organizations tend to take a more positive strategic view towards compliance with the PCI Data Security Standard. More than 2 out of 3 view PCI DSS as the best available framework to guide their implementations. In addition, about half see an opportunity to leverage cardholder data security achieved through PCI DSS compliance to drive better protection of other sensitive business data, and to address compliance with other standards and regulations. In contrast, more than 1 out of 3 Laggard organizations have adopted the strategy of doing the minimum required to satisfy the major payment card brands.

The payment card industry has made steady progress by first establishing a common set of security standards, then by a period of widespread evangelism and encouragement regarding adoption. The next phase will incorporate both encouragement as well as tighter enforcement, including potential fines or penalties (including higher interchange rates) associated with PCI DSS non-compliance. Companies that view PCI DSS as an opportunity, not as merely an obligation, are developing capabilities that can improve their business performance in addition to providing better protection for cardholder data.

In the next chapter, we describe what the top performers are doing to achieve superior protection of cardholder data.
Chapter Two: Benchmarking Requirements for Success

A clear understanding of the flow of cardholder data (e.g., cardholder name, primary account number, and expiration date) and sensitive authentication data (e.g., magnetic stripe data, PIN numbers, and card validation values) provides the initial foundation for implementing policies, business processes, and enabling technologies to achieve compliance with the PCI Data Security Standard and ultimately to derive broader business benefits.

<table>
<thead>
<tr>
<th>Case Study: Litle &amp; Co.</th>
</tr>
</thead>
</table>
| Litle & Co., a payment processor headquartered in Lowell, Massachusetts, first reported compliance in 2003 (at the time, with Visa’s Cardholder Information Security (CISP) program). Founded in 2001, Litle & Co. is the only independent payment processing company focused exclusively on direct commerce merchants (e.g., catalogers, direct marketers, e-tailers, and other non-face-to-face merchants). Early on, Litle & Company viewed compliance with industry security standards as much as a business opportunity as an obligation. “We viewed it as an opportunity for continuous improvement, not just for security but for our key business processes,” says David Kamins, Chief Technology Officer for Litle & Co. In the beginning, Kamins recalls that the rigor of the security standards was not viewed positively by everyone. “At first, we almost had mass mutiny from our developers, whose reaction was something like ‘we can’t work like this!’” Kamins notes. “But each year, we have systematically ratcheted in tighter and tighter controls. Looking back, I can’t think of a single case where we’ve said ‘that’s just not a reasonable requirement.’ In fact, we think some of them can still be tightened up a bit.” As a result of implementing better protections for cardholder data, Litle & Co. has realized not only better security, but also internal operating efficiencies and improvements in overall system reliability. One specific example of cost avoidance is that as the number of merchants serviced by Litle & Company has grown from 10 to over 600, the number of support staff has needed to grow by only 3 people. “Our process efficiencies have enabled us to scale transparently with the growth of the business,” Kamins notes, “while maintaining separation of duties between developers and support, and providing excellent levels of service to our customers.” Litle & Co. believes that the application of leading-edge technology and continuous improvement in their core business processes provides them with a technological edge over their competition and enables them to deliver the highest possible quality of service to its merchant customers. Litle & Co. was ranked Number 1 on the 2006 “Inc. 500” list with $34.8M in 2005 revenue and 3-year revenue growth of 5,629%.

Survey respondents fell into one of three categories – Best in Class, Industry Average, or Laggards – which displayed significantly different characteristics across five key areas: (1) Process (ability to identify

### Fast Facts
- Time to meet PCI DSS requirements was consistently estimated at between 12-18 months, independent of whether or not compliance had already been reported.
- Cost to meet PCI DSS requirements was consistently underestimated by those who have not reported compliance, compared with those who have (Industry Average underestimate by a factor of 1.4X, while Laggards underestimate by a factor of 3.5X).

© 2007 Aberdeen Group, Inc.  
www.aberdeen.com
vulnerabilities and assess risk in the cardholder data environment); (2) Organization (ownership and responsibility for key elements of cardholder data security); (3) Knowledge (thorough knowledge of cardholder data flow and elimination of cardholder data storage post-authorization); (4) Technology (selection and effective deployment of appropriate enabling technologies); and (5) Performance (ability to measure benefits of technology deployment and to use the results to further improve key business processes).

Table 3: Competitive Framework

<table>
<thead>
<tr>
<th>Process</th>
<th>Laggards</th>
<th>Industry Average</th>
<th>Best in Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Formal risk assessments for all system components in the cardholder data environment</td>
<td>14%</td>
<td>51%</td>
<td>68%</td>
</tr>
<tr>
<td>Vulnerability assessments for all system components in the cardholder data environment</td>
<td>17%</td>
<td>57%</td>
<td>79%</td>
</tr>
<tr>
<td>Comprehensive risk rating for all system components in the cardholder data environment</td>
<td>11%</td>
<td>27%</td>
<td>47%</td>
</tr>
<tr>
<td>Gap analysis (pre-assessment) comparing existing cardholder data security measures to the PCI Data Security Standard</td>
<td>14%</td>
<td>47%</td>
<td>68%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Organization</th>
<th>Laggards</th>
<th>Industry Average</th>
<th>Best in Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible executive or team with ownership for leading the PCI compliance effort</td>
<td>28%</td>
<td>63%</td>
<td>89%</td>
</tr>
<tr>
<td>Strict separation of duties, i.e., remediation and audit functions are performed by different people</td>
<td>36%</td>
<td>53%</td>
<td>63%</td>
</tr>
<tr>
<td>An internal audit team manages the audit and certification process</td>
<td>18%</td>
<td>46%</td>
<td>79%</td>
</tr>
<tr>
<td>A Qualified Security Assessor manages the audit and certification process</td>
<td>18%</td>
<td>31%</td>
<td>68%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Knowledge</th>
<th>Laggards</th>
<th>Industry Average</th>
<th>Best in Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprehensive data flow diagrams for cardholder data and sensitive authentication data</td>
<td>14%</td>
<td>31%</td>
<td>58%</td>
</tr>
<tr>
<td>No storage of cardholder data (e.g., cardholder name, primary account number, expiration date) post-authorization</td>
<td>25%</td>
<td>35%</td>
<td>47%</td>
</tr>
<tr>
<td>No storage of sensitive authentication data (e.g., magnetic stripe data, PIN numbers, card validation values) post-authorization</td>
<td>36%</td>
<td>48%</td>
<td>63%</td>
</tr>
<tr>
<td>Formal security awareness and training programs around PCI DSS</td>
<td>18%</td>
<td>29%</td>
<td>47%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technology</th>
<th>Laggards</th>
<th>Industry Average</th>
<th>Best in Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elimination or encryption of cardholder data within unstructured data files (e.g., in spreadsheets, word processing documents, local databases, etc.)</td>
<td>25%</td>
<td>43%</td>
<td>53%</td>
</tr>
<tr>
<td>Segmentation of the network to isolate systems that store, process or transmit cardholder data from those that do not</td>
<td>21%</td>
<td>42%</td>
<td>63%</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Performance</th>
<th>Laggards</th>
<th>Industry Average</th>
<th>Best in Class</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure network built and maintained</td>
<td>23%</td>
<td>74%</td>
<td>100%</td>
</tr>
<tr>
<td>Cardholder data protected during storage, processing and transmission</td>
<td>39%</td>
<td>61%</td>
<td>95%</td>
</tr>
<tr>
<td>Vulnerability management program established and maintained</td>
<td>7%</td>
<td>49%</td>
<td>68%</td>
</tr>
<tr>
<td>Strong access control mechanisms implemented</td>
<td>22%</td>
<td>53%</td>
<td>100%</td>
</tr>
<tr>
<td>Networks regularly monitored and tested</td>
<td>25%</td>
<td>67%</td>
<td>95%</td>
</tr>
<tr>
<td>Information security policy established and maintained</td>
<td>37%</td>
<td>70%</td>
<td>95%</td>
</tr>
</tbody>
</table>

Source: Aberdeen Group, June 2007
Organizational Capabilities and Technology Enablers

Once a clear strategic commitment to achieving PCI DSS compliance has been made, two other factors provide an indication of the alignment between an organization's strategy and execution of its PCI DSS compliance initiative: clear cross-functional ownership and responsibility, and adequate resource allocation.

As shown in Figure 2, more than 75% of Best in Class companies have assigned primary responsibility for their PCI DSS compliance initiative to either the CIO or to a dedicated PCI Compliance Manager or PCI Program Office. Best in Class companies are more likely than the Industry Average to have a dedicated PCI owner, by a factor of nearly 3X.

Figure 4: Primary Responsibility for Your PCI Compliance Initiative

With respect to budget, our research shows that the cost to meet the PCI DSS requirements was consistently underestimated by those who have not yet reported compliance, compared with estimates by those who have. Compared to Best in Class organizations, the Industry Average underestimate the total cost of their PCI Compliance initiatives by a factor of 1.4X, while Laggards underestimate total cost by a factor of 3.5X. Perhaps more telling, 79% of the Industry Average and 95% of Laggards indicate that their organizations have not fully budgeted their estimated total cost for addressing PCI DSS. This does not bode well for a dramatic increase in the percentage of organizations reporting PCI DSS compliance in the coming year.

Interestingly, the time to meet the PCI DSS requirements was consistently estimated at between 12-18 months, independent of whether or not compliance had already been reported.
Aberdeen Insights – Technology

Over the past 12 months, Best in Class companies have made the greatest strides in improving their performance in the following three PCI DSS requirements:

- Encrypt transmission of cardholder data across open, public networks (89% year-over-year performance improvement)
- Protect stored cardholder data (79% year-over-year performance improvement)
- Develop and maintain secure systems and applications (70% year-over-year performance improvement)

For the first two items, data encryption and key management have been key enabling technologies. For the third item, key enabling technologies include secure application development tools, application firewalls and gateways, and application vulnerability scanners.

Looking ahead to the next 12 months, based on year-over-year projected growth (planned use vs. current use) for all respondents, the enabling technologies with highest growth outlook include the following:

- Qualified Security Assessors (104%)
- Approved Scanning Vendors (103%)
- Aggregated log analysis, auditing and reporting (including SIM, SIEM) (88%)
- Application vulnerability scanners (56%)
- Data encryption (52%)

Services and policy-oriented enablers also show high growth potential in the next 12 months, including the following:

- Formal risk assessment (87%)
- Formal test plans for systems and processes (71%)
- Formal information security policy (37%)

Stepping back, given the current state of implementation it is no surprise to look for continued growth in the use of enabling technologies and services across all three phases of the typical PCI DSS compliance initiative: pre-assessment (understanding risks and gaps), remediation (implementing additional technologies, policies or procedures), and final assessment / audit.
Chapter Three: Required Actions

Whether a company is trying to move its performance in the protection of cardholder data from “Laggards” to “Industry Average,” or from “Industry Average” to “Best in Class,” the following actions will help spur the necessary performance improvements:

Laggards Steps to Success

- Follow the Data: develop comprehensive data flow diagrams for cardholder data and sensitive authentication data in your cardholder data environment.
- Mind the Gap: conduct a pre-assessment gap analysis (in house, or with an external consultant) comparing your existing cardholder data security measures to those specified by PCI Data Security Standard.
- Assign Clear Ownership: name a responsible executive or team with clear ownership and responsibility for leading your PCI compliance effort.
- Allocate the Resources: 95% of Laggards indicate that their organizations have not fully budgeted their estimated total cost for addressing PCI DSS.

Industry Norm Steps to Success

- Follow the Data: develop comprehensive data flow diagrams for cardholder data and sensitive authentication data in your cardholder data environment. Best in Class companies are 1.9X more likely than the Industry Average to have developed this capability.
- Assign Clear Ownership: name a responsible executive or team with clear ownership and responsibility for leading your PCI compliance effort. Best in Class companies are more likely than the Industry Average to have a dedicated PCI owner, by a factor of nearly 3X.
- Protect the Data: “protect stored cardholder data” and “encrypt transmission of cardholder data across open, public networks” were the top two areas of performance improvement by the Best in Class in the previous 12 months. The Industry Average performance in these areas is lower than the Best in Class by a factor of about 1.5X.
- Allocate the Resources: 79% of the Industry Average indicate that their organizations have not fully budgeted their estimated total cost for addressing PCI DSS.

Best in Class Steps to Success

- Continue Incremental Improvements: of the 12 high-level PCI DSS security requirements, those with greatest opportunity for improved performance are #2 (do not use vendor-supplied defaults for system
passwords and other security parameters), #7 (restrict access to cardholder data by business need-to-know), #10 (track and monitor all access to network resources and data), and #11 (regularly test security systems and processes).

- **Increase Awareness and Education:** although the scope of PCI DSS “touches everyone in the company”, only 47% of Best in Class companies currently conduct formal security awareness and training programs around PCI DSS.

### Aberdeen Insights – Summary

Public disclosures of security breaches involving consumer cardholder data are a threat to consumer confidence in payment cards and a growing financial drain on the payment card industry. By establishing a common set of security standards for the protection of cardholder data, the payment card industry aims to address both issues – and also to avoid potential regulatory actions under consideration by governments around the world.

Aberdeen research shows that Best in Class companies have indeed achieved superior protection of cardholder data through compliance with the Payment Card Industry (PCI) Data Security Standard (DSS). As the industry begins to shift from mere encouragement to enforcement – from soft-dollar “carrots” to hard-dollar “sticks” – for compliance, one would expect to see the percentage of organizations reporting compliance on the rise. Such a rise may be limited, however, by underfunding of the resources necessary for the overall PCI compliance effort, as indicated by the data.
Appendix A: 
Research Methodology

In June 2007, Aberdeen Group examined the protection of cardholder data in the payment card industry and the state of implementation of the Payment Card Industry (PCI) Data Security Standard (DSS). The experiences and intentions of more than 125 enterprises from a diverse set of industries are represented in this study.

Respondents completed an online survey that included questions designed to determine the following:

- The degree to which the 12 high-level security requirements of the PCI Data Security Standard have been implemented, and the motivations and obstacles to implementation over the past 12 months;
- The structure and effectiveness of existing PCI DSS implementations;
- Current and planned use over the next 12 months of key enabling technologies to aid in the achievement of PCI DSS compliance; and
- The benefits, if any, that have been derived from PCI DSS compliance initiatives.

Aberdeen supplemented this online survey effort with telephone and in-person interviews with select survey respondents, gathering additional information on strategies, experiences, and results related to protecting cardholder data and the implementation of the PCI Data Security Standard.

The study aimed to identify current and emerging best practices for protecting cardholder data and to provide a framework by which readers could assess their own organization’s capabilities.

Responding enterprises included the following:

- **Job title/function:** The research sample included respondents with the following job titles: CEO/President/COO/CIO/CFO/Chief Compliance Officer (24%); Vice President/Director (23%); Manager (31%); and Staff/Consultant/Other (22%). Areas of functional responsibility included: IT (39%); Finance (15%); Business Process Management (13%); Marketing/Sales (21%); and Customer Service/Other (12%).

- **Industry:** The research sample included respondents from a diverse range of industries. Retail, Finance, Travel/Hospitality/Restaurant, Apparel, and Food/Beverage represented more than 60% of the total. Respondents came from diverse mix of companies from within the payment card industry, including Merchants, Service Providers, Issuing/Acquiring Banks, and Payment Processors.

- **Geography:** The majority of respondents (71%) were from North America. Remaining respondents were from the Asia-Pacific region (11%), Europe/Middle East/Africa (15%), and South/Central America and the Caribbean (3%).
• **Company size:** 28% of respondents were from large enterprises (annual revenues above US$1 billion); 28% were from midsize enterprises (annual revenues between $50 million and $1 billion); and 44% of respondents were from small businesses (annual revenues up to $50 million).

Solution providers recognized as sponsors of this report were solicited after the fact and had no substantive influence on the direction of the *Protecting Cardholder Data* benchmark report. Their sponsorship has made it possible for Aberdeen Group to make these findings available to readers at no charge.

**Table 4: PACE Framework**

<table>
<thead>
<tr>
<th><strong>PACE Key</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Aberdeen applies a methodology to benchmark research that evaluates the business Pressures, Actions, Capabilities, and Enablers (&quot;PACE&quot;) that indicate corporate behavior in specific business processes. These terms are defined as follows:</td>
</tr>
<tr>
<td><strong>Pressures</strong> — external forces that impact an organization’s market position, competitiveness, or business operations (e.g., economic, political and regulatory, technology, changing customer preferences, and competitive pressures)</td>
</tr>
<tr>
<td><strong>Actions</strong> — the strategic approaches that an organization takes in response to industry pressures (e.g., align the corporate business model to leverage industry opportunities, such as product/service strategy, target markets, financial strategy, go-to-market, and sales strategy)</td>
</tr>
<tr>
<td><strong>Capabilities</strong> — the business process competencies required to execute corporate strategy (e.g., skilled people, brand, market positioning, viable products/services, ecosystem partners, financing)</td>
</tr>
<tr>
<td><strong>Enablers</strong> — the key functionality of technology solutions required to support the organization’s enabling business practices (e.g., development platform, applications, network connectivity, user interface, training and support, partner interfaces, data cleansing, and management)</td>
</tr>
</tbody>
</table>

Source: Aberdeen Group, June 2007

**Table 5: Maturity Class Framework**

<table>
<thead>
<tr>
<th><strong>Maturity Class Framework Key</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The Aberdeen Maturity Class Framework defines enterprises as falling into one of the following three levels of practices and performance:</td>
</tr>
<tr>
<td><strong>Best in Class (20%)</strong> — Practices in protecting cardholder data that are the best currently being employed and significantly superior to the industry average, and result in the top industry performance.</td>
</tr>
<tr>
<td><strong>Industry Average (50%)</strong> — Practices in protecting cardholder data that represent the industry average or norm, and result in average industry performance.</td>
</tr>
<tr>
<td><strong>Laggards (30%)</strong> — Practices in protecting cardholder data that are significantly behind the average of the industry, and result in below average performance.</td>
</tr>
</tbody>
</table>
Table 6: Relationship between PACE and Competitive Framework

Aberdeen research indicates that companies that identify the most impactful pressures and take the most transformational and effective actions are most likely to achieve superior performance. The level of competitive performance that a company achieves is strongly determined by the PACE choices that they make and how well they execute.

Source: Aberdeen Group, June 2007
Appendix B:
Related Aberdeen Research

Related Aberdeen research that forms a companion or reference to this report include:

- *Thwarting Data Loss: Best in Class Strategies for Protecting Sensitive Data* (May 2007)
- *Vulnerability Assessment: What You Don’t Know CAN Hurt You* (June 2007)
- *Developing Secure Applications* (June 2007)
- *Securing Deployed Applications* (June 2007)

Information on these publications and any other Aberdeen research can be found at [www.aberdeen.com](http://www.aberdeen.com).

Author: Derek E. Brink, Vice President & Research Director, IT Security ([Derek.Brink@aberdeen.com](mailto:Derek.Brink@aberdeen.com))

Founded in 1988, Aberdeen Group is the technology-driven research destination of choice for the global business executive. Aberdeen Group has over 100,000 research members in over 36 countries around the world that both participate in and direct the most comprehensive technology-driven value chain research in the market. Through its continued fact-based research, benchmarking, and actionable analysis, Aberdeen Group offers global business and technology executives a unique mix of actionable research, KPIs, tools, and services.

This document is the result of research performed by Aberdeen Group. Aberdeen Group believes its findings are objective and represent the best analysis available at the time of publication. Unless otherwise noted, the entire contents of this publication are copyrighted by Aberdeen Group, Inc. and may not be reproduced, stored in a retrieval system, or transmitted in any form or by any means without prior written consent by Aberdeen Group, Inc.