Payment Card Industry
Introduction
Introduction

Donald E. Hester
CISSP, CISA, CAP, MCT, MCITP, MCTS, MCSE Security, Security+
Maze & Associates, Director
@One / San Diego City College
www.LearnSecurity.org
http://www.linkedin.com/in/donaldhester
http://www.facebook.com/group.php?gid=245570977486
The Problem

Albert Gonzalez, 28

With accomplices, he was involved in data breaches of most of the major data breaches:
Heartland, Hannaford Bros., 7-Eleven, T.J. Maxx, Marshalls, BJ’s Wholesale Club, OfficeMax, Barnes & Noble, Sports Authority, Dave & Busters, Boston Market, Forever 21, DSW and others.
Alarming Trend

Number of incidents per year.

Source: [DATA LOSS db open security foundation](http://www.datalossdb.org)
Highest IT Priorities for 2008

1. Information Security Management
2. IT Governance
4. Privacy Management
5. Business Process Improvement, Workflow and Process Exceptions Alerts (new to list)
6. Identity and Access Management
7. Conforming to Assurance and Compliance Standards
8. Business Intelligence (new to list)
9. Mobile and Remote Computing
10. Document, Forms, Content and Knowledge Management

1, 2, 4, 6, & 7, are all PCI related

Source: AICPA’s 19th Annual Top Technology Initiatives survey
Highest IT Priorities for 2009

1. Information Security Management
2. Privacy Management
3. Secure Data File Storage, Transmission and Exchange
5. Mobile and Remote Computing
6. Training and Competency
7. Identity and Access Management
8. Improved Application and Data Integration
9. Document, Forms, Content and Knowledge Management
10. Electronic Data Retention Strategy

1, 2, 3, 6, 7, & 10, are all PCI related

Source: AICPA’s 20th Annual Top Technology Initiatives survey
Players

- **Acquirer (Merchant Bank)**
  - Bankcard association member that initiates and maintains relationships with merchants that accept payment cards

- **Hosting Provider**
  - Offer various services to merchants and other service providers.

- **Merchant**
  - Provides goods and services for compensation

- **Cardholder**
  - Customer to whom a card is issued or individual authorized to use the card
Players

- Card Brand
  - Issue fines
  - Determine compliance requirements
- PCI Security Standards Council
  - Maintain standards for PCI
  - Administer ASV & QSA
- Qualified Security Assessors
  - Certified to provide annual audits
- Approved Scanning Vendor
  - Certified to provide quarterly scans
PCI Council Standards
What is the PCI security standards council’s mission?
To maintain and update the Data Security Standard (PCI DSS) and to produce supporting documentation such as audit guidelines. From the PCI Council website: "The PCI Security Standards Council’s mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards."
Website

https://www.pcisecuritystandards.org/
What are the Standards?

• PCI DSS: PCI Data Security Standard
  – Overall standard, applies to all
• PA DSS: Payment Application Data Security Standard
  – Supporting standard for payment applications
• PTS (was PED): PIN Transaction Security Standard
  – Supporting standard for PIN entry devices
  – Supporting standard for unattended payment terminals (UPT)
PCI DSS

• The Payment Card Industry Data Security Standard
• 6 Objectives (Goals)
• 12 Sections (Requirements)
• 194 Controls

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 1.2
October 2008
The standard has approximately 194 controls in 12 sections. The 12 sections are group into 6 objectives. The 6 objectives are; build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, maintain an information security policy.
Standard Lifecycle

1. Market Implementation (10/1/08 – 6/30/09)
2. Feedback Begins (7/1/09 – 10/31/09)
3. Feedback Review and Decision (11/1/09 – 4/30/10)
5. Discuss New Version / Revision (9/30/10)
Who must comply?

- With PCI DSS
  - Any organization the processes, stores or transmits credit card information.
- With PA DSS
  - Payment application developers
  - Merchants will be required to use only compliant applications by July 2010.
- With PTS
  - Manufactures of PIN entry devices
  - Merchants will be required to use only compliant hardware by July 2010.
  - MasterCard PTS to incorporate into PCI SSC April 30, 2010

This includes organizations who only use paper based processing, organizations who outsource the credit card processing, to organizations that process credit cards in house.
PCI Compliance

- This includes:
- Organizations who only use paper based processing
- Organizations who outsource the credit card processing
- Organizations that process credit cards in house
Is PCI law?

- The PCI DSS was developed by the payment card brands
- Compliancy is compulsory if a merchant wishes to continue processing payment card transactions
- However, some States have enacted legislation that has made PCI compliance the law
What if we are a small organization?

- “All merchants, whether small or large, need to be PCI compliant.
- The payment brands have collectively adopted PCI DSS as the requirement for organizations that process, store or transmit payment cardholder data.”
  — PCI SSC
If there is a data breach, the card brands will perform a forensic audit to determine if the merchant was compliant at the time of the data breach. If the merchant is found not compliant at the time of the breach they will be liable for the full cost of the breach; the cost of the forensics, losses of cardholders, losses to the banks, losses to the card brand and in some states fines will be assessed. In addition, the merchant will be moved to the highest merchant level and will be required to meet the most stringent evidence requirements and their credit card processing fees will go up.
What’s Safe Harbor?

http://usa.visa.com/merchants/risk_management/cisp_if_compromised.html
Safe Harbor Notes:

• For a merchant to be considered compliant, any Service Providers that store, process or transmit credit card account data on behalf of the merchant must also be compliant.

• The submission of compliance validation documentation alone does not provide the merchant with safe harbor status.
Outside the Safe Harbor

- Losses of cardholders
- Losses of banks
- Losses of card brands
  - Fines from the Card brands
  - Possible restrictions on process credit cards
  - Cost of forensic audit
Fines

Merchants may be subject to fines by the card associations if deemed non-compliant. For your convenience fine schedules for Visa and MasterCard are outlined below.

<table>
<thead>
<tr>
<th>Visa Fine Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Violation</td>
</tr>
<tr>
<td>Second Violation</td>
</tr>
<tr>
<td>Third Violation</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Visa’s PCI Compliance Acceleration Program (PCI CAP) Fine Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
</tr>
<tr>
<td>Level 2</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MasterCard Assessment Schedule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
</tr>
<tr>
<td>Level 2</td>
</tr>
<tr>
<td>Level 3</td>
</tr>
</tbody>
</table>

PCI DSS

- The Payment Card Industry Data Security Standard
- 6 Objectives (Goals)
- 12 Sections (Requirements)
- 194 Controls

Payment Card Industry (PCI) Data Security Standard

Requirements and Security Assessment Procedures
Version 1.2
October 2008
The standard has approximately 194 controls in 12 sections. The 12 sections are group into 6 objectives. The 6 objectives are; build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, maintain an information security policy.
PCI DSS

- Start implementing the data security standard starting with policies
- Start with high level policies
  - “The City shall not store PAN (Credit Card Numbers) electronically or physically. Employees shall be trained on PCI standard annually. Background checks will be performed on all staff with access to credit card information.”
Create Needed Policies

• What policies do you currently have that address PCI related issues
• Create needed policies
• See section 12 of the PCI DSS
• You will need to create additional subordinate policies, procedures or administrative directives for specific PCI control requirements
• Every PCI DSS control should be documented in some policy, procedure, administrative directive, SOP or schedule
PII Policy

- If you already have a policy for handling confidential information or personally identifiable information add credit card information to confidential information or PII.
PCI DSS

- Use the prioritized approach to implement the most important controls first.

<table>
<thead>
<tr>
<th>Requirement 1: Install and maintain a firewall configuration to protect cardholder data.</th>
<th>Milestone</th>
<th>Status: Please enter &quot;yes&quot; if fully compliant with the requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1 Establish firewall and router configuration standards that include the following:</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1.1.3 Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>1.1.4 Description of groups, roles, and responsibilities for logical management of network components</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>1.1.6 Requirement to review firewall and router rule sets at least every six months</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>
Each merchant is placed in levels based upon the number of transactions they process. These levels determine what evidence of compliance must be submitted. (Validation Requirements)

Merchants with a low number of transactions can complete self-assessment questionnaire.

Merchants in the middle submit questionnaires and have external scans.

At the highest level merchants must have a full independent audit and external scan.

**Merchant Levels**

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>E-commerce transactions</th>
<th>All other transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Over 6 million annually</td>
<td>Over 6 million annually</td>
</tr>
<tr>
<td>Level 2</td>
<td>1 to 6 million annually</td>
<td>1 to 6 million annually</td>
</tr>
<tr>
<td>Level 3</td>
<td>20,000 to 1 million annually</td>
<td>N/A</td>
</tr>
<tr>
<td>Level 4</td>
<td>Up to 20,000 annually</td>
<td>Up to 1 million annually</td>
</tr>
</tbody>
</table>

Merchant levels are determined by the annual number of transactions *not* the dollar amount of the transactions.
Validation Requirements

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>QSA Audit</th>
<th>Quarterly Network Scans</th>
<th>Self-Assessment Questionnaire</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Level 2</td>
<td>*</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Level 3</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Level 4</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Separate and distinct from the mandate to comply with the PCI DSS is the validation of compliance whereby entities verify and demonstrate their compliance status.

* Starting 12-31-2010 MasterCard will require Annual QSA Audits for Level 2 Merchants

External Scans by an Approved Scanning Vendor (ASV), at least quarterly
Annually fill out Self Assessment Questionnaire (SAQ)
Even if your bank has not requested one
If level 1 or 2 you will need an audit from a Qualified Security Assessor (QSA)
Continuous Process

• “PCI DSS compliance is much more than a “project” with a beginning and end – It’s an ongoing process of assessment, remediation and reporting” - PCI SSC
Continuous Process

- Many of the PCI requirements have specific time interval requirements
- Create a schedule for time based requirements
- Some organizations already have ‘maintenance calendars’ for these type of actions
Common Findings

• Clients think they are compliant
  – Because they do quarterly networks scans
  – Because they filled out the SAQ
  – Because they have too few transactions
• Reality
  – Validation is not compliance
  – Compliance is an ongoing process
  – PCI DSS is required for all merchants, regardless of the number of transactions
Common Findings

- Payment card information on paper
- No network segmentation
- Logging Access
- Shared Passwords
- Verifying compliance of outsourced processing
- No one is assigned responsibility
- Not aware of PAN storage in application
PCI Pitfalls

- PCI will not make an organization’s network or data secure
- PCI DSS focuses on one type of data: payment card transactions
- The organization runs the risk of focusing on one class of data to the detriment of everything else
Payment Card Industry (PCI) Introduction

Updated April 2010
Contents
Introduction to PCI ................................................................. 2
Merchant Levels........................................................................ 2
Validation Requirements .......................................................... 2
Self Assessment Questionnaires ................................................. 3
Quarterly Network Scans ............................................................ 3
Additional Standards ................................................................. 4
Safe Harbor ............................................................................... 4
Frequently Asked Questions (FAQ's) .............................................. 6
Resources .................................................................................. 7
Definitions ................................................................................. 7
About the Author ....................................................................... 8
Disclaimer .................................................................................. 8
Introduction to PCI
All organizations that process payment cards (Visa, MasterCard, AMEX, etc...) have to comply with the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS was developed by the payment card brands and compliance is essential if a merchant wishes to continue processing payment card transactions. This includes merchants that only use paper-based processing, merchants that outsource the credit card processing, and merchants that process credit cards in-house.

The PCI DSS has approximately 194 controls in 12 sections, and the 12 sections are grouped into 6 objectives. The 6 objectives are: build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy. The first step in complying with the PCI DSS is filling out a Self Assessment Questionnaire (SAQ). In February 2008, the PCI Council announced different validation types for merchants, depending upon the risk of the processing environment. Merchants who outsource processing have 11 questions to attest to, while merchants who process transactions in-house on custom applications have to attest to all 226 questions.

Each merchant is placed in levels based upon the number of transactions processed. These levels determine what evidence of compliance must be prepared and whether it is necessary to submit the documentation to the merchant’s acquiring bank (Referred to as Merchant Bank or Acquirer). Merchants with a low number of transactions need to only complete the SAQ and maintain the documentation in-house. Merchants in the middle levels must submit the SAQs and evidence of performing external scans to their acquiring banks. At the highest level, merchants must have an external scan and a full independent PCI audit by a Qualified Security Assessor (QSA).

Merchant Levels
Merchant levels are determined by the annual number of transactions not the dollar amount of the transactions.

<table>
<thead>
<tr>
<th>Merchant Level</th>
<th>E-commerce transactions</th>
<th>All other transactions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1</td>
<td>Over 6 million annually</td>
<td>Over 6 million annually</td>
</tr>
<tr>
<td>Level 2</td>
<td>1 to 6 million annually</td>
<td>1 to 6 million annually</td>
</tr>
<tr>
<td>Level 3</td>
<td>20,000 to 1 million annually</td>
<td>N/A</td>
</tr>
<tr>
<td>Level 4</td>
<td>Up to 20,000 annually</td>
<td>Up to 1 million annually</td>
</tr>
</tbody>
</table>

Merchant levels are defined by each of the card brands and determined by your Acquirer (Merchant Bank). Each card brand has different level definitions. The definitions in this graph represent those of MasterCard and Visa. If you have a significant number of American Express, JCB or Discover Card transactions contact your Acquirer for assistance in determining your merchant level.

Validation Requirements
Separate and distinct from the mandate to comply with the PCI DSS is the validation of compliance whereby entities verify and demonstrate their compliance status. The merchant level of the entities determines what the organization must do to validate their compliance with PCI DSS. Compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants depending on your Acquirer (Merchant Bank).
* Starting December 31, 2010 MasterCard will require Annual QSA Audits for Level 2 Merchants.

**Self Assessment Questionnaires**
The Payment Card Industry Security Standards Council (PCS SSC) revised the original version of the Self Assessment Questionnaire (SAQ) in February 2008 in order to address the various scenarios that can exist at a merchant’s point of sale environment. As most Acquirers (Merchant Banks) require Self Assessment Questionnaires on merchant levels 2, 3 and 4, it is important to know which version of the SAQ your business may need to complete.

There are five SAQ validation categories. Use the table below to select which SAQ applies to your business.

<table>
<thead>
<tr>
<th>SAQ Validation Type</th>
<th>Description</th>
<th>SAQ</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.</td>
<td>A</td>
</tr>
<tr>
<td>2</td>
<td>Imprint-only merchants with no electronic cardholder data storage</td>
<td>B</td>
</tr>
<tr>
<td>3</td>
<td>Stand-alone dial-up terminal merchants, no electronic cardholder data storage</td>
<td>B</td>
</tr>
<tr>
<td>4</td>
<td>Merchants with payment application systems connected to the Internet, no electronic cardholder data storage</td>
<td>C</td>
</tr>
<tr>
<td>5</td>
<td>All other merchants (not included in descriptions for SAQs A-C above) and all service providers defined by a payment brand as eligible to complete an SAQ.</td>
<td>D</td>
</tr>
</tbody>
</table>

**Quarterly Network Scans**
To demonstrate compliance with the PCI DSS, merchants and service providers may be required to have periodic PCI Security Scans conducted as defined by each payment card company. The PCI DSS requires that all merchants with externally-facing IP addresses perform external network scanning to achieve compliance. Acquirers (Merchant Banks) require the quarterly submission of scan reports for Level 1, 2 and 3 merchants and may require submission of scan reports by level 4 merchants. These scans are automated, non-intrusive web scans performed by a PCI Approved Scanning Vendor (ASV). The scans are scans conducted over the Internet by an ASV to evaluate your web perimeter for any known vulnerabilities.

---

1 For information on the different SAQ forms please see [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)
2 For a list of PCI Approved Scanning Vendors please see [https://www.pcisecuritystandards.org](https://www.pcisecuritystandards.org)
“PCI Security Scans may apply to all merchants and service providers with Internet-facing IP addresses. Even if an entity does not offer Internet-based transactions, other services may make systems Internet accessible. Basic functions such as e-mail and employee Internet access will result in the Internet-accessibility of a company’s network. Such seemingly insignificant paths to and from the Internet can provide unprotected pathways into merchant and service provider systems and potentially expose cardholder data if not properly controlled.”
- PCI DSS Security Scanning Procedures v 1.1

Additional Standards
Payment Application Data Security Standard (PA DSS) and the PIN Transaction Security (PTS) standard support the PCI DSS and address security of applications and hardware used to process payment card transactions.

“PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS.”
- Payment Card Industry Security Standards Council

“The PCI PED3 security alignment initiative is aimed at ensuring that the cardholder’s PIN, and any sensitive information such as resident keys, are protected consistently at a PIN acceptance device. The objective of the requirements is the provision of a single, consistent, and stringent standard for all PIN acceptance devices worldwide.”
- Payment Card Industry Security Standards Council

These supporting standards are aimed at vendors who are creating applications and hardware devices used in the processing of payment cards. By July 2010, Merchants will be required to use only compliant applications and hardware.

Safe Harbor
Safe harbor is the outcome of the PCI certification process and provides protection from fines and compliance exposure in the event of a data compromise. If there is a data breach, the card brands will perform a forensic audit to determine if the organization was PCI DSS compliant at the time of the data breach.

If the organization is found to be out of compliance at the time of the breach they may be liable for the full cost of the breach including the cost of the forensics, losses of cardholders, losses to the banks, losses to the card brand and in some states fines will be assessed. In addition, the organization will be moved to the highest merchant level and will be required to meet the most stringent evidence requirements and the credit card processing fees will increase.

To obtain safe harbor status a merchant must maintain full compliance at all times, including at the time of the breach as demonstrated during a forensic investigation. Notes: 1.) For a merchant to be considered compliant, any Service Providers that store, process or transmit credit card account data on behalf of the merchant must also be compliant. 2.) The submission of compliance validation documentation alone does not provide the member safe harbor status.

3 As of May 1, 2010 PIN Entry Device PED has been renamed to PIN Transaction Security PTS in order to accommodate the future, more broad, addition of other hardware interaction devices.
Frequently Asked Questions (FAQ's)

What is the PCI security standard council?
In response to large losses suffered because of data breaches of credit card information, the five major card brands formed the PCI Council. The council is not a legislative or government body.

Who are the five major card brands?
American Express, Discover, JCB, MasterCard, and Visa

What is the PCI security standards council's mission?
To maintain and update the Data Security Standard (PCI DSS) and to produce supporting documentation such as audit guidelines. From the PCI Council website: “The PCI Security Standards Council’s mission is to enhance payment account data security by fostering broad adoption of the PCI Security Standards.”

Who must comply?
Any organization the processes, stores or transmits credit card information. This includes organizations that only use paper based processing, organizations that outsource the credit card processing, to organizations that process credit cards in house.

What must they comply with?
The Payment Card Industry Data Security Standard (PCI DSS). The standard has approximately 194 controls in 12 sections. The 12 sections are group into 6 objectives. The 6 objectives are; build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, maintain an information security policy.

What are merchant levels?
Each merchant is placed in levels based upon the number or dollar amount of transactions they process. These levels determine what evidence of compliance must be submitted. Merchants with a low number of transactions can complete self-assessment questionnaire. Merchants in the middle submit questionnaires and have external scans. At the highest level merchants must have a full independent audit and external scan.

What is the self-assessment questionnaire (SAQ)?
Merchants have different levels of SAQ, depending upon the risk of the processing environment. Merchants who outsource processing or have paper only processing have less questions to answer. Merchants who process in house on custom application have to answer all the questions.

Do merchants have to be compliant only with the questions on the SAQ?
No merchants must comply with all of the PCI DSS. The questions on the SAQ only reflect the controls with the highest risk based upon the merchants processing environment. (Controls can be N/A depending upon the merchant’s environment)

Who do your report PCI compliance to?
The merchant/acquiring bank will inform their merchants of the level and required process for turning in evidence. Each bank is slightly different in the process and most are focusing on merchants with high volume and working their way down to the lowest volume merchants.
What is the cost of non-compliance?
Merchants who have not demonstrated compliance with PCI DSS by turning in their annual SAQ, vulnerability scan and/or audit will eventually be assessed higher processing rates for credit card transactions.

When will the higher rates be assessed?
Currently the card brands are rolling out the higher fees phased in over time starting with merchants with the highest level of transactions.

What happens when there is a data breach?
If there is a data breach, the card brands will perform a forensic audit to determine if the merchant was compliant at the time of the data breach. If the merchant is found not compliant at the time of the breach they will be liable for the full cost of the breach; the cost of the forensics, losses of cardholders, losses to the banks, losses to the card brand and in some states, fines will be assessed.

In addition, the merchant will be moved to the highest merchant level and will be required to meet the most stringent evidence requirements and their credit card processing fees will go up.

Is PCI compliance law?
The PCI DSS was developed by the payment card brands and compliancy is compulsory if a merchant wishes to continue processing payment card transactions. However, some States have enacted legislation that has made PCI compliance the law.

Resources
- PCI Security Standards Council
- Visa CISP program [www.visa.com/cisp](http://www.visa.com/cisp)
- MasterCard SDP (Site Data Protection) Program [https://sdp.mastercardintl.com](https://sdp.mastercardintl.com)
- GFOA Recommended Practice, [Acceptance of Credit and Debit Cards](https://gfoa.gatech.edu/programs/credit-debit-cards), 22 FEB 2008

Definitions
- AFD: Automated Fuel Dispensers
- ASV: Approved Scanning Vendor
- CHD: Cardholder Data
- CISP: Cardholder Information Security Program (Visa)
- DISC: Discover Information Security & Compliance (Discover)
- DSE: Data Security Entity
- DSOP: Data Security Operating Policy (American Express)
- EPP: Encrypting PIN Pad
- JCB DSP: JCB Data Security Program (JCB)
- MOTO: Mail Order Telephone Order
- PA DSS: Payment Application Data Security Standard
- PABP: Payment Application Best Practices
- PAN: Primary Account Number
- PA QSA: Payment Application Qualified Security Assessor
- PCI: Payment Card Industry
- PCI CAP: Visa’s PCI Compliance Acceleration Program
- PCI DSS: Payment Card Industry Data Security Standard
- PCI SSC: Payment Card Industry Security Standards Council
PED  PIN Entry Device
PIN  Personal Identification Number
POS  Point of Sale
PSP  Payment Service Provider
PTS  PIN Transaction Security
QSA  Qualified Security Assessor
ROC  Report on Compliance
SAQ  Self Assessment Questionnaire
SDP  Site Data Protection (MasterCard)
TPP  Third Party Providers
UPT  Unattended Payment Terminal
VNP  VisaNet Processor
VPA  Validated Payment Applications

About the Author
Donald E. Hester
Donald's clients include local municipalities, non-profits, corporations and federal government agencies, specializing in a wide array of compliance programs and security assessments such as PCI, FISMA, COBIT and ISO17799. He is a Guest lecturer and speaker on security topics and he has served on various advisory committees and as a Subject Matter Expert in Information Technology and Security. Donald received his bachelors, with honors, in Security Management with a concentration in Information Security from American Military University. He has over 15 years of experience in the security field. His certifications include; CISSP, CISA, CAP, PSP, MCT, MCTIP, MCSE Security, MCSA Security, MCTS, MCDST, Security+ and CTT+. Donald also teaches Microsoft and information security courses at San Diego City College and for the California State Chancellor's office.

Donald's LinkedIn Profile: http://www.linkedin.com/in/donaldehester

Disclaimer
This document contains a compilation of information received from various sources. This information is presented solely for the convenience of the reader and should not be used as a substitute for your own research and reference to actual regulations and/or other official documents, or as a substitute for consulting your legal advisor. Maze & Associates is not responsible for inaccurate, outdated, or incomplete information. All information contained herein is subject to change.