



Payment Card Industry Data Security Standard

Office of the State Treasurer

Ryan Pitroff

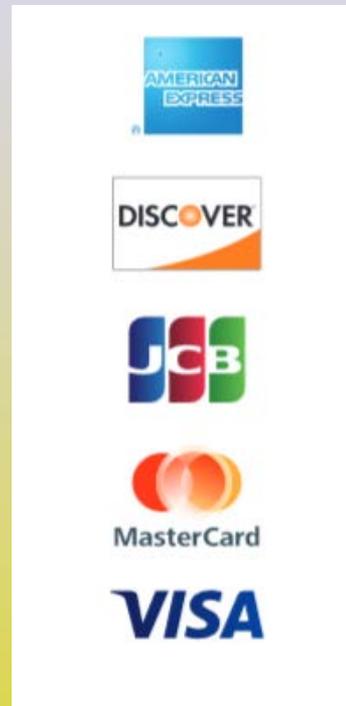
Banking Services Manager

Ryan.Pitroff@tre.wa.gov



PCI-DSS

- A common set of industry tools and measurements to help ensure the safe handling of sensitive information.
- Developed and managed by the PCI Security Standards Council
- Applies to all merchants and third party service providers that
 - Store/Process/Transmit Card Holder Data
 - Develop/ Sell Payment Applications





PCI-DSS Summarized

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored cardholder data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software or programs6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need to know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security for all personnel



PCI Compliance Levels

Level 1

Merchants processing over 6 million card transactions annually (all channels) or Global merchants identified as Level 1 by any Visa region

- Annual Report on Compliance (“ROC”) by Qualified Security Assessor (“QSA”) or Internal Auditor
- Quarterly network scan by Approved Scan Vendor (“ASV”)
- Attestation of Compliance Form

Level 2

Merchants processing 1 million to 6 million card transactions annually (all channels)

- Annual Self-Assessment Questionnaire (“SAQ”)
- Quarterly network scan by ASV
- Attestation of Compliance Form

Level 3

Merchants processing 20,000 to 1 million e-commerce transactions annually

- Annual SAQ
- Quarterly network scan by ASV
- Attestation of Compliance Form

Level 4

Merchants processing less than 20,000 e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually

- Annual SAQ recommended
- Quarterly network scan by ASV if applicable
- requirements set by merchant bank



Self Assessment Questionnaires (SAQs)

SAQ A	Card not present merchants (ecommerce or mail/telephone order) that have fully outsourced all cardholder data functions to PCI DSS compliant third party service providers, with no electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Not applicable to face to face channels
SAQ A-EP	Ecommerce merchants who outsource all payment processing to PCI DSS validated third parties, and who have a website(s) that doesn't directly receive cardholder data but that can impact the security of the payment transaction. No electronic storage, processing, or transmission of any cardholder data on the merchant's systems or premises. Applicable only to e-commerce channels.
SAQ B	Merchants using only <ul style="list-style-type: none">•Imprint machines with no electronic cardholder data storage; and/or•Standalone, dial out terminals with no electronic cardholder data storage. Not applicable to e-commerce channels



Self Assessment Questionnaires (SAQs)

SAQ B-IP	Merchants using only standalone, PTS-approved payment terminals with an IP connection to the payment processor, with no electronic cardholder data storage. Not applicable to e-commerce channels.
SAQ C-VT	Merchants who manually enter a single transaction at a time via a keyboard into an Internet based virtual terminal solution that is provided and hosted by a PCI DSS validated third-party service provider. No electronic cardholder data storage. Not applicable to e-commerce channels
SAQ C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage. Not applicable to e-commerce channels.
SAQ P2PE-HW	Merchants using only hardware payment terminals that are included in and managed via a validated, PCI SSC-listed P2PE solution, with no electronic cardholder data storage. Not applicable to e-commerce channels
SAQ D	All merchants not included in descriptions for the above SAQ types



Cost of Non Compliance

- If a merchant is found to be non-compliant they can be fined up to \$25,000 per month.
- Noncompliance assessments will begin 1 January 2015 for noncompliant or overdue level 1 and level 2 merchants
- Visa may impose additional measures including, but not limited to, risk reduction requirements, disconnection from VisaNet, and agent disqualification.
- In case of a breach, merchants will be assessed the cost to notify and reissue cards for affected cardholders. This can be \$100 to \$300 per record compromised.



PCI-DSS Case Study

- Entity Profile:** Accepts Bankcards in-person at multiple locations. Has a website with online acceptance of bankcards that they outsourced to a 3rd party to manage. Classified as a level 2 merchant
- Challenges:** Multiple Challenges, from project management issues, to incomplete gap analysis, all pointing to a lack of understanding of the PCI-DSS
- Solution(s):** Still a Work in Progress, but getting better.



PCI-DSS Case Study

Project Management Issues

- Ownership of the process – No one wanted to take the job
- Gave the job to an accountant with no prior PM experience, and very little bankcard experience
- Were unable to get resources from their 3rd party vendor to assist in analyzing the vendor's side of things.
- Project Manager got busy with day to day issues and put the project on the back burner



PCI-DSS Case Study

Incomplete Gap Analysis

- Inability to engage internal IT resources
- Inability to engage 3rd party IT resources
- Guessing at answers instead of digging deeper and knowing the answers
- Lacked a clear understanding of the relationship of their internal systems, and how those interfaced with the 3rd party system(s)
- Completely missed the fact that their 3rd party was retaining full card data



PCI-DSS Case Study

Lack of Understanding of PCI-DSS

- Through this process it became apparent that this agency did not understand PCI-DSS or the implications of being in non-compliance with the standard
- Even though it was communicated early and often, they missed their compliance deadline and then had to request an extension
- It was only when they were under the threat of having merchant services turned off did they comprehend the seriousness of the issue



PCI-DSS Case Study

Solutions

- Engage and get buy in from executive management
 - *Agency assigned an effective Project Manager*
 - *Agency management staff were told to drop everything and assist the PM whenever questions needed to be answered*
- Fully vet your business process
 - *First thing the PM did was a full analysis of their entire business process, from initial card acceptance through settlement*
 - *During this analysis it was discovered they had a requirement of their vendor to retain full card data*



PCI-DSS Case Study

Solutions

- Get outside help when needed
 - *Hired a Qualified Security Assessor (QSA)*
 - *After identifying full card data was being kept, analyzed their business need for that data and determined it was in their best interest to not retain full card numbers.*
- Complete your PCI-DSS Validation timely
 - *Because this agency was so late in validating their compliance, our Acquirer looked it over much more closely than normal. This took extra resources to answer their many and varied probing questions*
- Start working on next year's validation early



PCI-DSS Case Study

Solutions

- Make sure the correct SAQ is being done
If you are accepting in-person transactions only with hardware terminals, the validation of your compliance requirements will look much different than a merchant who has online acceptance or who retains card data
- Make sure your contracts with 3rd party vendors address your data security requirements
- Don't Retain Card Data
If you have a business need to retain full card data, do what you can to change that process. If you still have the need, find a solution that will best protect you from a data breach



PCI-DSS Resources

PCI Data Security Standard (PCI DSS)

www.pcisecuritystandards.org

The Standard:

https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf

Supporting Documents:

https://www.pcisecuritystandards.org/security_standards/documents.php

Approved Assessors and Scanning Vendors:

https://www.pcisecuritystandards.org/approved_companies_providers/index.php

Self-Assessment Questionnaires:

https://www.pcisecuritystandards.org/merchants/self_assessment_form.php