

Industry Members:



©digitalcommunities™

# Everything You Need to Know About Payment Card Industry Compliance in Government



# Everything You Need to Know About Payment Card Industry Compliance in Government

## Introduction

Government agencies are increasingly offering more online services as a way to reduce costs and improve constituent interactions. In 2010, a Pew Research Center survey found that 83 percent of respondents had looked for information or completed a transaction on a government website the prior year – the amount of online transactions has continued to increase since then.<sup>1</sup> As with any online transaction, the biggest concern is always security. How can government agencies ensure they are properly protecting cardholder data, and most importantly, instilling trust in constituents so they continue to complete transactions online? The answer is to comply with Payment Card Industry (PCI) Security Standards. This paper provides valuable information to government agencies about the complicated topic of PCI compliance so they can benefit from online transactions without the risk of non-compliance.

## PCI Security Standards: What They Are and How They Are Managed

The PCI Security Standards have both technical and operational requirements. The standards complement each other and apply to all entities that accept, store, process or transmit cardholder data, including government agencies. The standards also provide guidance for software developers and manufacturers of applications and equipment used in credit card transactions.

The standards include:

- PCI PIN Transaction Security – for card swipe equipment manufacturers
- PCI Payment Application Data Security Standard – for software development companies writing payment applications

- PCI Data Security Standard – for merchants, service providers<sup>2</sup> and any entity which accepts, transmits or otherwise handles cardholder data

The most current version, PCI Security Standard 2.0, was issued in October 2010. The PCI Security Standards Council is presently in the second year of a three-year review cycle – a revision of the standard is in progress and is expected in 2013.

The PCI Security Standards Council (PCI-SSC or simply the “Council”) was launched in 2006 by five major companies that issue credit cards and process payments.<sup>3</sup> PCI-SSC is responsible for the development and management of the PCI Security Standards as well as outreach, education and awareness programs for merchants. Global payment companies – specifically the founding Council members – have security compliance programs which incorporate PCI-SSC’s security standards and other technical requirements. Each company’s program and reporting requirements will vary, but all are based upon the PCI Security Standards. Requirements are enforced through affiliated card-issuing banks and other payment processors. The banks and payment processors in turn enforce the requirements with their customers – merchants and government agencies that accept cards and electronic payments.

## Why is Compliance So Critical for Government?

The PCI Security Standards are *not* government-mandated. They are comprised of standards and guidelines set by the private PCI Security Standards Council.

At least one state, Nevada, now legally requires that local governments comply with PCI guidelines.<sup>4</sup> But even without a state law,

## Resources

- PCI Security Standards, [www.pcisecuritystandards.org/security\\_standards/](http://www.pcisecuritystandards.org/security_standards/)
- Hitchhiker’s Guide to PCI DSS 2.0 Scoping by Steve Levinson, <http://networkingexchangeblog.att.com/enterprise-business/hitchhikers-guide-to-pci-dss-2-0-scoping-part-1/>
- Compliance Requirements for the PCI Data Security Standard, Quest Software, [www.quest.com/Quest\\_Site\\_Assets/PDF/DSW-CompliancePCIUS-FINAL\\_02122009.pdf](http://www.quest.com/Quest_Site_Assets/PDF/DSW-CompliancePCIUS-FINAL_02122009.pdf)
- Jackson’s Identity Management & Active Directory Reality Tour Travelblog, <http://jacksonshaw.blogspot.com/>
- McAfee Blog Central by Kim Singletary, <http://blogs.mcafee.com/author/kim-singletary>
- T. J. Maxx Data Breach, [www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm](http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm)

## Endnotes

1. “How Americans Interact with Government Online,” Pew Research Center, <http://pewresearch.org/pubs/1575/how-americans-interact-with-government-online>
2. A service provider typically provides card validation, storage, transmission and similar services to merchants and government agencies. Examples include NIC Inc., and Paypal.
3. American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.
4. This is Nevada law NRS 603A. Nevada was the first state to require compliance, according to Laura Fucci, former CIO of Clark County, Nev.
5. See, for example, the May 2012 breach in Utah, where 800,000 constituent records were exposed, [www.govtech.com/policy-management/Utah-CIO-Steve-Fletcher-Resigns-State-Promises-Security-Reforms.html](http://www.govtech.com/policy-management/Utah-CIO-Steve-Fletcher-Resigns-State-Promises-Security-Reforms.html)
6. Adapted from the PCI Standards 12 Steps
7. Card Verification Value – typically a three or four digit number found on the card but not part of the card number itself.
8. Also note that a single incident of loss of cardholder data in this fashion might cause breach reporting and similar mitigations to occur for *all* transactions that an employee processed over a considerable period of time.
9. Ibid.
10. T. J. Maxx had a serious breach due to this flaw in 2007, with perhaps 94 million Visa and MasterCard accounts compromised, and losses projected to approach \$4.5 billion, [www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm](http://www.nysscpa.org/cpajournal/2008/808/essentials/p34.htm)
11. Cardholder Data Environment – the systems, storage, applications and networks which process or transmit card holder data.
12. For a more detailed look at this, consult Steve Levinson’s four-part series “A Hitchhiker’s Guide to PCI DSS 2.0 Scoping,” <http://networkingexchangeblog.att.com/enterprise-business/hitchhikers-guide-to-pci-dss-2-0-scoping-part-1/>
13. “Mobile devices present a special challenge,” says David Moody, Vice President, KANA. “We need applications which don’t require the cardholder data to reside in the mobile phone or tablet, because so many are unprotected by passwords and easily stolen.”

By Bill Schrier, director of the *Digital Communities* program, with the assistance of the Digital Infrastructure Task Force.

The Center for Digital Government and *Government Technology* would like to thank the *Digital Communities* Digital Infrastructure Task Force members for their support and assistance in the creation of this report, with special recognition to the following task force members and interviewees for their contributions.

**Jayne Friedland Holland** – Association General Counsel and Chief Security Officer, NIC Inc.

**Jeffrey Falcon CISSP** – CIPP/US, Senior Security Solutions Architect, CDW-Government

**Steve Levinson** – PCI Practice Director, AT&T Consulting

**Kim Singletary** – Director of Technical Solutions Marketing, McAfee

**David Moody** – Vice President, Product Marketing, KANA

**Jackson Shaw** – Senior Director, Product Development, Quest Software

**Laura Fucci** – CIO of Henderson, Nev., and former CIO of Clark County, Nev.

## Protection of Cardholder Payment Data



Ecosystem of payment devices, applications, infrastructure and users

Source: Adapted from NIC, Inc.

## What's a Government to Do?

Many city, county and state governments may already be accepting credit and debit card payments and partially complying with PCI standards. But no matter what stage you're in, here's a quick checklist to get you on the road to PCI compliance:

- ✓ Don't rely on hope (as in hoping that your agency won't have a breach).
- ✓ Don't stick your head in the sand and assume someone else in the organization is worrying about PCI compliance.
- ✓ Find the individuals in your organization responsible for payment processing; these will often include the treasurer or chief financial officer and may include a chief information security officer (CISO) or equivalent.
- ✓ Find the appropriate contact at your service provider or acquiring issuer (bank) and obtain checklists or forms which they use to determine PCI compliance for their merchants.
- ✓ Determine all the ways your organization accepts card payments today and who in each business unit is primarily responsible for these business processes.
- ✓ Make sure you identify all systems and networks which touch cardholder data and the CDE,<sup>11</sup> and keep the CDE to the minimum necessary size.<sup>12</sup>
- ✓ Form a council of the individuals above to work through the PCI compliance process and checklists.
- ✓ Engage skilled and certified third-party consultants or expertise to assist in and verify the work. "PCI Compliance is a million shades of grey, not black-and-white," says AT&T's Levinson. A qualified security assessor can help you sort through those "shades of grey."

Fucci recommends that every agency have a policy and procedure for dealing with breaches. "With the handling of HIPAA and PCI and CJIS and personal information ... it is best to have an established process so you can handle the decision-making and next steps, should a breach occur."

Payment card brands are responsible for the enforcement of PCI compliance, as well as assessing fines and penalties in the event of non-compliance. While their fines are not widely publicized, payment brands may fine an acquiring bank (and ultimately the merchant) \$5,000 to \$100,000 for PCI compliance violations. According to Friedland Holland, "It's important for all merchants (including government) to understand its agreement with its acquiring bank in order to be aware of the liability should a breach occur. For example, at NIC all merchant services agreements are provided to NIC's internal legal counsel for a review of any and all obligations between the parties, including the indemnification obligations in the event of a security breach."

## The Future

A variety of standards and technology changes are in progress today which will affect PCI compliance. These include:

- the upcoming Version 3.0 of the PCI standards;
- new mobile applications on a variety of platforms — Android, Windows 8, iPhone and perhaps Blackberry — which present new challenges to PCI compliance both for the applications and the devices;<sup>13</sup>
- tablet computing and access to payment websites via tablet applications;
- new networking technologies such as RFID and Near-Field Communication (NFC);
- continuing changes in Web browsers and their capabilities; and
- continuing challenges from hackers, criminal syndicates and even nation-states which attempt to exploit every software and human vulnerability.

## Conclusion

Compliance with the PCI standards is critical for every government agency that accepts credit and debit cards for payment. The risk of a breach and subsequent loss of PII would lessen citizen confidence and could result in fines. While PCI compliance can be complicated, costly and onerous, an agency can use a number of techniques such as engaging competent, qualified PCI compliance consultants to support its efforts. A thorough compliance program will pay dividends both in the short term and long term.

the PCI guidelines carry great weight because failure to comply and the loss of cardholder data have significant and onerous consequences for any merchant, including government agencies.

Loss — even potential loss — of cardholder information triggers automatic reporting of the breach to both private and government regulators. Such loss can force a government agency to purchase expensive credit monitoring and other services for the affected cardholders. According to Kim Singletary, director of technical solution marketing at McAfee, "Banks will refuse to process payments from violators and the agency may not be able to accept credit or debit cards for payments. Remediation will require third-party assessment and probably means higher fees from the merchant's credit card service provider."

Additionally, any potential exposure or loss of constituent personally identifiable information (PII) such as card information shakes the confidence of constituents in their government. Such breaches could have disastrous effects<sup>5</sup> for both senior officials such as CIOs and elected officials such as mayors, governors and legislators.

Because of the consequences, compliance with the PCI security standards is essentially required of any government agency that accepts electronic payments through debit or credit cards, whether over the counter, via telephone, through a website or by any other means. The exception is that transactions such as direct debits from bank accounts or loyalty cards are not subject to PCI security standards.

## What is Required of Government to Comply?

Below is a list of some of the most common requirements and suggestions to build and maintain PCI compliance.<sup>6</sup>

- Write and enforce a strong information security policy, and educate the workforce about the policy.
- Install and maintain firewalls to protect the applications and databases or systems which contain or transmit cardholder data.
- Assign unique user IDs for every individual in the agency who has computer or system access.
- Enforce and regularly change *strong* passwords for applications, servers, systems and individuals involved in any aspect of card processing. Protect any system or database that stores cardholder data, or, preferably, outsource all such storage to a trusted third-party service provider.
- Restrict access to cardholder data only to individuals who must have that access.
- Encrypt transmission of cardholder data across open, public networks, or, ideally, any network.

## Identifying the Players and Roles

### PAYMENT BRANDS

American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

### CARDHOLDERS

Business or consumer customers to whom a payment card is issued, or any individual authorized to use the payment card.

### ISSUERS

Entities that issue payment cards or that perform, facilitate or support issuing services such as issuing banks and issuing processors. Issuers are sometimes called the "issuing financial institution."

### MERCHANTS

Any entity that accepts payment cards as payment for goods and/or services, including governments. With PCI, government agencies are treated just like any other merchant such as a department store, retail shop or online retailer.

### ACQUIRERS

Entities (usually banks) that merchants use to authorize and process their payment card transactions. Acquirers communicate to issuers and receive authorization to allow a transaction to occur. They then provide clearing and settlement services to merchants.

### SERVICE PROVIDERS

Business entities directly involved in the processing, transmitting or storage of cardholder data in support of a merchant. In certain situations, merchants may also be considered service providers.

### COMPLIANCE ROLES

The Council also sets requirements for and certifies companies and individuals in roles that help educate merchants and enforce the PCI standards. Some of these roles are:

- Qualified Security Assessors (QSA)
- Payment Application Qualified Security Assessor (PA-QSA)
- Approved Scanning Vendors (ASV)

- Use and regularly update anti-virus software on all systems and servers which touch cardholder data.
- Develop and maintain secure systems and applications; ideally this includes review and evaluation of the application code by a qualified third-party security firm.
- Restrict physical access to cardholder data, e.g. to call centers or over-the-counter payment processing areas.
- Track and monitor all access to computer systems, applications, network resources and cardholder data.
- Regularly test security systems and processes.
- Engage an approved scanning vendor to conduct regular external network vulnerability scans of all websites which accept cardholder data; scans must be performed quarterly.
- Consider conducting pre-employment police background checks for all employees who may potentially handle cardholder data.
- Train and regularly refresh the training of all employees who are involved in handling cardholder data.

Although governments can't entirely outsource their PCI compliance requirements, they can engage service providers to handle transaction processing. However, it is important to ensure that these providers are certified. According to Jayne Friedland Holland, associate general counsel and chief security officer at NIC Inc., governments should always, "outsource to a qualified service provider that has been PCI SSC certified through a qualified security assessor or QSA. In fact, government should always require a certificate of PCI compliance from any third-party vendor it uses."

Since governments can't outsource all PCI compliance requirements, they still need to train employees that handle credit card information. Jackson Shaw, senior product development manager at Quest Software, says, "There are many examples where a network administrator or systems administrator did not properly secure the network or a server, allowing a breach of identity and potentially cardholder information."

Steve Levinson, PCI practice director at AT&T Consulting, adds, "Ultimately the burden is on the merchant/service provider to secure that [cardholder] information."

Laura Fucci, CIO of Henderson, Nev., and former CIO of Clark County, Nev., adds that scanning for vulnerabilities is key to maintaining PCI compliance. She tracks four tests required by PCI:

- Internal Scans — quarterly and after significant change in network
- External Scans — quarterly and after significant change in network; must be performed by approved scanning vendor (ASV)
- Application Penetration Test — annual and after any

significant change in infrastructure or application; must be performed by qualified internal resource or qualified external third party

- Network Penetration Test — annual and after significant change in infrastructure or application; must be performed by qualified internal resource or qualified external third party

### Validating PCI Compliance

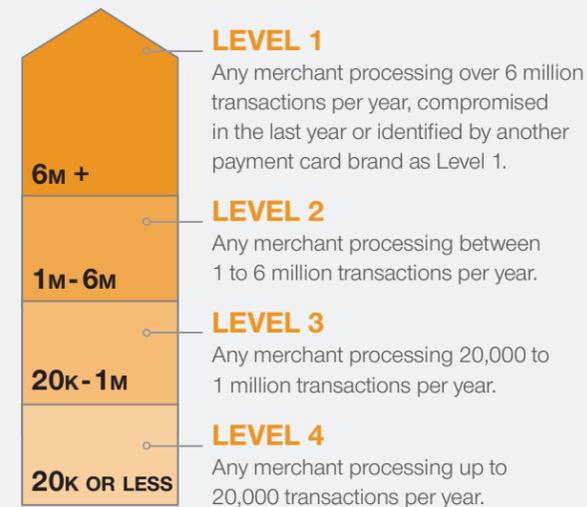
Validation requirements will vary based upon level. At Level 1, for example, the merchant or government agency must have a council-validated qualified security assessor (QSA) company perform an assessment and write a report of compliance (ROC).

All other levels can perform a self-assessment utilizing the self-assessment forms published by PCI SSC. Both types of assessment must be accompanied by an Attestation of Compliance form signed by an executive officer of the company or government.

Also, each merchant and service provider, no matter what level, must have external quarterly vulnerability scans run by a PCI SSC validated ASV.

### Determining Merchant Levels

As a government agency processes more transactions, the risk of breach or compromise of cardholder data also increases. Consequently, the compliance and validation requirements become more stringent. Merchant levels are based on volume of transactions. The levels are defined by the payment brands, but the actual level for any particular merchant or government agency will be determined by its acquiring bank(s). Typical levels are:



### The PCI Compliance Challenges

One of the main challenges that government faces with PCI compliance is the cost. NIC's Friedland Holland states that based on a recent study, "a compliance effort could take 6 to 18 months; cost over \$100,000 in consulting and up to \$500,000 in system, software and infrastructure upgrades."

These costs are influenced by a variety of factors, including engagement of competent, certified service providers to manage most of the processing, storage and management of electronic payments.

In an effort to achieve PCI compliance, governments can seek guidance from the acquiring bank that is responsible for merchant compliance, as well as reporting compliance status to the credit card companies. Governments may also consider engaging a company with PCI compliance expertise rather than attempting such an effort alone.

Another common challenge is the time associated with complying. PCI compliance requires a thorough examination of entire business processes. Take, for example, payment of water utility bills. The business process examination would probably include:

- Presenting methods for accepting card payments:
  - On paper through the mail
  - Over the counter in a payment center
  - Over the telephone by a customer service agent
  - Over the telephone via an interactive voice response (IVR) system
  - Over the Web
  - Via a mobile (smartphone or tablet) payment application
- Examining all the individuals involved who talk to customers or might see or handle cardholder data in person, over the phone or by another means
- Examining all applications, systems, networks, Web functions and similar automated systems where cardholder data might be stored or through which such data might be transmitted (This step is critical, according to Jeff Falcon, senior security solutions architect with CDW-G, as it defines the cardholder data environment. "There is a misconception that everything on the network must be PCI compliant, but that's not true," Falcon says. "Only those systems and networks which touch cardholder data are subject to PCI.")
- Reviewing the crediting process where overpayments or mistaken payments are applied back to a cardholder's account

Henderson CIO Fucci emphasizes the importance of defining the cardholder data environment (CDE). She advises segmenting the environment so that any systems that handle card transactions



are in a separate segment than the rest of the computing environment. The PCI assessment would then need to occur only on the segment. "We have been working towards segmentation for years and getting the applications moved to the separate segment has not been easy," she says. "Our ultimate goal is to stop processing payment transactions altogether on county assets." She advises leveraging a third-party payment processor to handle the transactions, and not allowing this sensitive data on government systems or networks.

### The Consequences of Non-Compliance

The most common consequences of non-compliance that a government would face are a data breach and subsequent fine. A breach is any loss or unauthorized access to cardholder data. Cardholder data includes the cardholder name, card number, CVV<sup>7</sup> code, expiration date, PIN and related information. Breaches, or potential breaches include:

- employees in call centers who lose or steal and use constituent cardholder information,<sup>8</sup> perhaps simply by writing it down on a piece of paper and carelessly discarding that paper;
- employees in over-the-counter payment functions (parks community centers, permit desks, driver's license offices, etc.) who lose or steal and use cardholder information;<sup>9</sup>
- stolen or lost laptops, thumb drives and other media which contains the cardholder data, even if the data is not used criminally;
- compromise of a database, server storage or similar repository which contains cardholder data — such compromise might be copying the data by someone who is not authorized to handle or manage the data through a stolen or lost password to the repository; and
- network scanning through, for example, an open WiFi network where unencrypted transactions are observed on the open network.<sup>10</sup>