

Five Myths About the Payment Card Industry Data Security Standard

By Walt Conway

It was inevitable. Governments, businesses, hospitals, and universities nationwide are working to comply with the Payment Card Industry Data Security Standard (PCI DSS). Unfortunately, these entities sometimes get misleading advice or simply wrong information. The purpose of this article is to dispel five common myths surrounding PCI compliance. These five myths can waste valuable time and resources or, more seriously, leave you vulnerable to a security breach.

PCI DSS was created to protect cardholder data. If you are a merchant that stores, processes, or transmits cardholder data, you must comply with the standard. This means that the growing number of state, county, and municipal governments accepting payment (i.e., credit and debit) cards for fees, fines, or services is included. It also means that all payment channels (whether face-to-face, mail, fax, or e-commerce) are within scope of PCI DSS.

Myth 1: “I've outsourced my card processing, so I'm PCI compliant.” If only it were this easy. Outsourcing your card processing to a third-party can simplify your compliance effort. It can be a great strategy with a good partner. However, outsourcing by itself is not enough to make you compliant.

First confirm that your vendor is PCI compliant. If the vendor is not, you need to re-think the relationship. After that, remember you are still the merchant. You receive and process cardholder data when you print daily transaction summaries, receive reports from your processor, or process chargebacks. You likely have stacks of paper receipts containing card numbers. You still have some compliance work to do.

The good part is that outsourcing can make PCI compliance easier. Your compliance effort then can focus on policies and procedures.

Conclusion: Outsourcing has advantages, but it is not a panacea. If you decide to outsource major parts of your card processing, be sure to verify that your vendor or application is PCI compliant.

Payment Application Best Practices (PABP) and Compliant Service Providers

Visa developed a set of Payment Application Best Practices (PABP) to encourage software vendors to develop secure payment applications. If you need, say, a parking lot or event management application, you can check [this list](#) to find software solutions that will not prevent you from becoming PCI compliant.

Using a PABP application does not by itself assure a merchant of achieving compliance. It still has to be installed and maintained properly. The list is version-specific, so be sure you are installing the correct, PABP-certified version. Finally, being on this list says nothing about the software's functionality, only that the application meets the PABP criteria.

Soon the PABP will migrate from Visa to the PCI Security Standards Council where it will be folded into the standard. It will then be re-named PA DSS to reflect the change.

Service providers must have their PCI compliance validated by a qualified, outside assessor. Use [this list of compliant service providers](#) to find PCI compliant third-party payment application service providers.

Myth 2: “PCI compliance is just another Information Technology (IT) project.” This myth reflects a misunderstanding of the risks involved. First, PCI compliance is not a “project” with a start and finish date. Rather, it is a process (some call it a journey) that requires ongoing commitment and resources. Second, compliance is a *business* issue (not merely a technology issue) that affects the entire government. The risks of a data compromise are both financial and reputational as noted in the recent *Treasury Management Newsletter* article, [“The Payment Card Industry Data Security Standard: Where to Begin.”](#)

PCI compliance calls for a multidisciplinary approach including both treasury and IT—and often your audit, legal, and purchasing departments, too.

Conclusion: Compliance is a business issue affecting the entire government. While IT has an important role, it is not the only—or necessarily even the lead—player.

Myth 3: “I’m a small merchant, so I only have to meet some PCI requirements.” Every merchant has to comply with all the requirements regardless of their size. The only difference is how you validate compliance.

You are assigned a merchant level based on your card activity. The largest,

Level 1 merchants generally need to file a Report on Compliance validated by an outside qualified security assessor (these are vetted by the PCI Council). Level 2, 3, and 4 merchants can self-assess their compliance. Either way, each merchant must meet each of the requirements in the standard. The big difference is that if you are a Level 1 merchant, it will cost you more to validate your compliance.

Conclusion: PCI compliance is “pass/fail.” You need to meet all the requirements no matter how big or small a merchant you are. By the way, *if you suffer a security breach, you will be moved to Level 1 regardless of your transaction volume.*

Self-Assessment Questionnaire for PCI Compliance

The self-assessment questionnaire is a tool used by merchants to self-validate their PCI compliance. There are [four versions of the self-assessment questionnaire](#). Which one is right for you depends on how you process payment cards.

Self-Assessment Questionnaire Type	Description	# of Questions to be Answered
A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	11
B	Imprint-only merchants with no electronic cardholder data storage; and stand-alone terminal merchants, no electronic cardholder data storage	24
C	Merchants with point-of-sale systems connected to the Internet, no electronic cardholder data storage	32
D	All other merchants	226 (Full DSS)

Merchants not storing cardholder data electronically are eligible for Self-Assessment Questionnaire Types A, B, and C, which are shorter and easier to complete than Type D. So your choice is either don't keep cardholder data or expect to spend a lot of time answering questions.

Myth 4: “PCI DSS is unreasonable with inflexible requirements.” PCI is a prescriptive standard. This means it specifies both what is to be achieved

and how it is to be done. As a result it is easy to be overwhelmed by the volume of PCI documents and supporting material. A closer look, though, will show that PCI contains nothing that is not a best practice already. Its elements are familiar to finance and IT professionals. Governments practicing good security will find they already meet most PCI requirements.

In a situation where for good business reasons you cannot implement a control requirement in the manner specified, you may implement a “compensating control” to satisfy the requirement by other means. The key to developing a compensating control is to focus on the intent of the original control requirement, and then show how the original objective is accomplished by other means.

Conclusion: There is nothing alien or even particularly new in the PCI standard. The option of using “compensating controls” provides merchants some flexibility in meeting the standard.

Myth 5: “The card industry requires me to keep cardholder data.” This is perhaps the biggest and most stubborn myth of all. You do not need to store cardholder data anywhere in your government. There is no requirement to store cardholder data from either PCI or the card brands (American Express, Discover, JCB, MasterCard, and Visa). The payment card industry actually is doing everything in its power to discourage you from retaining cardholder data.

We have to distinguish between payment data and cardholder data. You need to keep payment information including the transaction date, amount, and the last 4 digits of the card (which are not “cardholder data”). If there is a disputed transaction, you have enough information to work with your processor to resolve the dispute.

The new self-assessment questionnaires reinforce your not storing cardholder data, particularly electronically. If you qualify to use one of the simpler versions, you will simplify your PCI compliance greatly.

Conclusion: You do not need to retain cardholder data. Your PCI mantra should be: “If you don't need it, don't keep it.”

There is one final point about PCI DSS. By implementing these security practices you will create business processes that will serve your government well across all your operations. Therefore achieving PCI compliance is not only a requirement, it makes good business sense.

Walt Conway is an independent e-commerce consultant based in San Francisco who conducts

PCI training and edits the PCI blog for the Treasury Institute for Higher Education; he also is the National Association of College and University Business Officers representative to the PCI Security Standards Council. (www.walterconway.com).

[Top](#)

Useful Resources on PCI Compliance

Treasury Management Newsletter

- [The Payment Card Industry Data Security Standard: Where to Begin](#)

Blogs, Wikis, and Forums

- [Introduction to PCI DSS](#)
- [PCI Compliance Guide](#)
- [Treasury Institute PCI blog](#)
- [PCI Answers.com](#)

Card Associations

- [PCI Security Standards Council](#)
- [Visa](#)
- [Mastercard](#)
- [Discover](#)

Other Resources

- [Data Security Breaches: Context and Incident Summaries](#)
(Congressional Research Service Report for Congress) (This is an excellent summary of recent security breaches.)
- [PCI Compliance for Higher Education: Best Practices Checklist](#)
- [PCI Self Assessment Questionnaire](#)
- [Sample Job Description: PCI/DSS Compliance Officer](#)

[Top](#)

Cash Management Sessions at the GFOA Annual Conference

The upcoming GFOA conference in Fort Lauderdale, Florida on June 15–18, 2008, will include the following sessions related to investing and treasury management. More information on the conference is available on the [GFOA Web site](#).

- **How Safe Are Money Market Funds?** Almost 40 years ago, when money market funds were invented, investors flocked to them for better