

# PCI Facts and Myths

## PCI Facts:

### Q: What is PCI?

**A:** The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that **process, store or transmit** credit card information maintain a secure environment. Essentially any merchant that has a Merchant ID (MID).

The Payment Card Industry Security Standards Council (PCI SSC) was launched on September 7, 2006 to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with focus on improving payment account security throughout the transaction process. The PCI DSS is administered and managed by the PCI SSC ([www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)), an independent body that was created by the major payment card brands (Visa, MasterCard, American Express, Discover and JCB.).

It is important to note, the payment brands and acquirers are responsible for enforcing compliance, not the PCI council.

A copy of the PCI DSS is available [here](#).

### Q: To whom does PCI apply?

**A:** PCI applies to ALL organizations or merchants, regardless of size or number of transactions, that accepts, transmits or stores any cardholder data. Said another way, if any customer of that organization ever pays the merchant directly using a credit card or debit card, then the PCI DSS requirements apply.

### Q: Where can I find the PCI Data Security Standards (PCI DSS)?

**A:** The Standard can be found on the PCI SSC's Website:

[https://www.pcisecuritystandards.org/security\\_standards/pci\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml)

### Q: What are the PCI compliance deadlines?

**A:** All merchant that stores, processes or transmits cardholder data must be compliant now. However, as a Level 4 merchant, you will have to refer to your merchant bank for their specific validation requirements and deadlines. All deadline enforcement will come from your merchant bank. You may also find more information on Visa's Website:

[http://usa.visa.com/download/merchants/payment\\_application\\_security\\_mandates.pdf](http://usa.visa.com/download/merchants/payment_application_security_mandates.pdf).

### Q: What are the PCI compliance 'levels' and how are they determined?

**A:** All merchants will fall into one of the four merchant levels based on Visa transaction volume over a 12-month period. Transaction volume is based on the aggregate number of Visa transactions (inclusive of credit, debit and prepaid) from a merchant Doing Business As ('DBA'). In cases where a merchant corporation has more than one DBA, Visa acquirers must consider the aggregate volume of transactions stored, processed or transmitted by the corporate entity to determine the validation level. If data is not aggregated, such that the corporate entity does not store, process or transmit cardholder data on behalf of multiple DBAs, acquirers will continue to consider the DBA's individual transaction volume to determine the validation level.

Merchant levels as defined by Visa:

Merchant Level	Description
1	Any merchant -- regardless of acceptance channel -- processing over 6M Visa transactions per year. Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.
2	Any merchant -- regardless of acceptance channel -- processing 1M to 6M Visa transactions per year.
3	Any merchant processing 20,000 to 1M Visa e-commerce transactions per year.
4	<b>Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants -- regardless of acceptance channel -- processing up to 1M Visa transactions per year.</b>

*\* Any merchant that has suffered a hack that resulted in an account data compromise may be escalated to a higher validation level.*

Source: [http://usa.visa.com/merchants/risk\\_management/cisp\\_merchants.html](http://usa.visa.com/merchants/risk_management/cisp_merchants.html)

### Q: What does a small-to-medium sized business (Level 4 merchant) have to do in order to satisfy the PCI requirements?

**A:** To satisfy the requirements of PCI, a merchant must complete the following steps:

- Identify your Validation Type as defined by PCI DSS – see below . This is used to determine which Self Assessment Questionnaire is appropriate for your business.

SAQ Validation Type	Description	SAQ
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. <i>This would never apply to face-to-face merchants.</i>	A
2	Imprint-only merchants with no cardholder data storage	B
3	Stand-alone dial-up terminal merchants, no cardholder data storage	B
4	Merchants with payment application systems connected to the Internet, no cardholder data storage	C
5	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.	D

- Complete the Self-Assessment Questionnaire according to the instructions in the Self-Assessment Questionnaire Instructions and Guidelines.
- Complete and obtain evidence of a passing vulnerability scan with a PCI SSC Approved Scanning Vendor (ASV). **Note** scanning does not apply to all merchants. It is required for Validation Type 4 and 5 – those merchants with external facing IP addresses. Basically if you electronically store cardholder information or if your processing systems have any internet connectivity, a quarterly scan by an approved scanning vendor is required.
- Complete the relevant Attestation of Compliance in its entirety (located in the SAQ tool).
- Submit the SAQ, evidence of a passing scan (if applicable), and the Attestation of Compliance, along with any other requested documentation, to your acquirer.
- I'm a small merchant with very few card transactions; do I need to be compliant with PCI DSS?

All merchants, 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.

**Q: If I only accept credit cards over the phone, does PCI still apply to me?**

**A:** Yes. All business that store, process or transmit payment cardholder data must be PCI Compliant.

**Q: Do organizations using third-party processors have to be PCI compliant?**

**A:** Yes. Merely using a third-party company does not exclude a company from PCI compliance. It may cut down on their risk exposure and consequently reduce the effort to validate compliance. However, it does not mean they can ignore PCI.

**Q: My business has multiple locations, is each location required to validate PCI Compliance?**

**A:** If your business locations process under the same Tax ID, then typically you are only required to validate once annually for all locations. And, submit quarterly passing network scans by an PCI SSC Approved Scanning Vendor (ASV), if applicable.

**Q: Are debit card transactions in scope for PCI?**

**A:** In-scope cards include any debit, credit, and pre-paid cards branded with one of the five card association/brand logos that participate in the [PCI SSC](#) - American Express, Discover, JCB, MasterCard, and Visa International.

**Q: Am I PCI compliant if I have an SSL certificate?**

**A:** No. SSL certificates do not secure a Web server from malicious attacks or intrusions. High assurance SSL certificates provide the first tier of customer security and reassurance such as the below, but there are other steps to achieve PCI Compliance.

- A secure connection between the customer's browser and the web server
- Validation that the Website operators are a legitimate, legally accountable organization

**Q: What are the penalties for noncompliance?**

**A:** The payment brands may, at their discretion, fine an acquiring bank \$5,000 to \$100,000 per month for PCI compliance violations. The banks will most likely pass this fine on downstream till it eventually hits the merchant. Furthermore, the bank will also most likely either terminate your relationship or increase transaction fees. Penalties are not openly discussed nor widely publicized, but they can be catastrophic to a small business.

It is important to be familiar with your merchant account agreement, which should outline your exposure.

**Q: What is defined as 'cardholder data'?**

**A:** Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, social security number, etc. All personally identifiable information associated with the cardholder that is stored, processed, or transmitted is also considered cardholder data.

**Q: What is the definition of 'merchant'?**

**A:** For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers

Source: PCI SSC

**Q: What constitutes a Service Provider?**

**A:** Any company that stores, processes, or transmits cardholder data on behalf of another entity is defined to be a Service Provider by the Payment Card Industry (PCI) guidelines.

**Q: What constitutes a payment application?**

**A:** What constitutes a payment application as it relates to PCI Compliance? The term payment application has a very broad meaning in PCI. A payment application is anything that stores, processes, or transmits card data electronically. This means that anything from a Point of Sale System (e.g., Verifone swipe terminals, ALOHA terminals, etc.) in a restaurant to a Website e-commerce shopping cart (e.g., CreLoaded, osCommerce, etc) are all classified as payment applications. Therefore any piece of software that has been designed to touch credit card data is considered a payment application.

**Q: What is a payment gateway?**

**A:** Payment Gateways connect a merchant to the bank or processor that is acting as the front-end connection to the Card Brands. They are called gateways because they take many inputs from a variety of different applications and route those inputs to the appropriate bank or processor. Gateways communicate with the bank or processor using dial-up connections, Web-based connections or privately held leased lines.

**Q: How is IP-based POS environment defined?**

**A:** The point of sale (POS) environment refers to a transaction that takes place at a merchant location (i.e. retail store, restaurant, hotel, gas station, convenience store, etc.). An Internet protocol (IP) -based POS is when transactions are stored, processed, or transmitted on IP-based systems or systems communicating via TCP/IP.

**Q: What is PA-DSS and PABP?**

**A:** PA-DSS refers to Payment Application Data Security Standard maintained by the PCI Security Standards Council. PABP is Visa's Payment Application Best Practices, which is now referred to as PA-DSS. Visa started the program and it is being transitioned to the PCI Security Standards Council (PCI SSC). To address the critical issue of payment application security, in 2005 Visa created the Payment Application Best Practices (PABP) requirements to ensure vendors provide products which support merchants' efforts to maintain PCI DSS compliance and eliminate the storage of sensitive cardholder data. See [www.visa.com/pabp](http://www.visa.com/pabp) for more information.

The Payment Card Industry Security Standards Council (PCI SSC) will maintain the PA-DSS and administer a program to validate payment applications' compliance against this standard. The PCI SSC now publishes and maintains a list of PA-DSS validated applications. See [https://www.pcisecuritystandards.org/security\\_standards/pa\\_dss.shtml](https://www.pcisecuritystandards.org/security_standards/pa_dss.shtml) for more information.

**VISA MANDATE PHASE DEADLINE**

1. New PCI Level 4 merchants (including new locations of existing relationships) may not use vulnerable payment application versions – those that store prohibited cardholder data. January 1, 2008
2. New PCI Level 4 merchants using third-party payment software must be either PCI DSS-compliant or use PA-DSS validated compliant payment applications. October 1, 2008
3. ALL PCI Level 4 merchants (new and existing) using third-party software must use validated applications. July 1, 2010

**Q: Can the full credit card number be printed on the consumer's copy of the receipt?**

**A:** PCI DSS requirement 3.3 states "Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed)." While the requirement does not prohibit printing of the full card number or expiry date on receipts (either the merchant copy or the consumer copy), please note that PCI DSS does not override any other laws that legislate what can be printed on receipts (such as the U.S. Fair and Accurate Credit Transactions Act (FACTA) or any other applicable laws). See the italicized note under PCI DSS requirement 3.3 "Note: This requirement does not apply to employees and other parties with a specific need to see the full PAN, nor does the requirement supersede stricter requirements in place for displays of cardholder data (for example, for point of sale (POS) receipts)." Any paper receipts stored by merchants must adhere to the PCI DSS, especially requirement 9 regarding physical security.

Source: PCI SSC

**Q: Do I need vulnerability scanning to validate compliance?**

**A:** If you electronically store cardholder data post authorization or if your processing systems have any internet connectivity, a quarterly scan by a PCI SSC Approved Scanning Vendor (ASV) is required.

**Q: What is a network security scan?**

**A:** A network security scan involves an automated tool that checks a merchant or service provider's systems for vulnerabilities. The tool will conduct a non-

intrusive scan to remotely review networks and Web applications based on the external-facing Internet protocol (IP) addresses provided by the merchant or service provider. The scan will identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company's private network. As provided by an Approved Scanning Vendors (ASV's) such as ControlScan the tool will not require the merchant or service provider to install any software on their systems, and no denial-of-service attacks will be performed.

Note, typically only merchants with external facing IP address are required to have passing quarterly scans to validate PCI compliance. This is usually merchants completing the SAQ C or D version.

**Q: How often do I have to scan?**

**A:** Every 90 days/once per quarter you are required to submit a passing scan. Merchants and service providers should submit compliance documentation (successful scan reports) according to the timetable determined by their acquirer. Scans must be conducted by a PCI SSC Approved Scanning Vendor (ASV). ControlScan is a PCI Approved Scanning Vendor.

**Q: What if a merchant refuses to cooperate?**

**A:** PCI is not, in itself, a law. The standard was created by the major card brands such as Visa, MasterCard, Discover, AMEX, and JCB. At their acquirers/service providers discretion, merchants that do not comply with PCI DSS may be subject to fines, card replacement costs, costly forensic audits, brand damage, etc., should a breach event occur.

For a little upfront effort and cost to comply with PCI, you greatly help reduce your risk from facing these extremely unpleasant and costly consequences.

**Q: If I'm running a business from my home, am I a serious target for hackers?**

**A:** Yes, home users are arguably the most vulnerable simply because they are usually not well protected. Adopting a 'path of least resistance' model, intruders will often zero-in on home users - often exploiting their 'always on' broadband connections and typical home use programs such as chat, Internet games and P2P files sharing applications. ControlScan's scanning service allows home users and network administrators alike to identify and fix any security vulnerabilities on their desktop or laptop computers.

**Q: What should I do if I'm compromised?**

**A:** We recommend following the procedures outlined in Visa's "What to Do If Compromised Visa Fraud Control and Investigations Procedures" document. Link below.

[http://usa.visa.com/download/merchants/cisp\\_what\\_to\\_do\\_if\\_compromised.pdf](http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf)

**Q: Do states have laws that requiring data breach notifications to the affected parties?**

**A:** Absolutely. California is the catalyst for reporting data breaches to affected parties. The state implemented breach notification law in 2003 and there are now over 38 states that have similar laws in place. See [www.privacyrights.org](http://www.privacyrights.org) for more detail on state laws.

## PCI Myths:

(Source: PCI Security Standards Council – PCI SSC)

**Myth: I'm a small merchant who only takes a handful of cards, so I don't need PCI.**

**Fact:** This is a common misunderstanding with the standard, that small merchants handling only one or a few credit cards a year are exempt from compliance. If you are a merchant and are set up to take credit cards by any mechanism - then you need to be compliant.

**Myth: PCI only applies to e-commerce companies.**

**Fact:** No, PCI applies to every company that stores, processes or transmits cardholder information. In fact anyone who takes card present transactions that involve POS devices are typically more at risk than e-commerce solutions. Quite often these types of transactions involve storage of track data (which is forbidden under PCI). Compromise of this type of data may bring heavy fines and requests for compensation from the banks involved.

**Myth: You only have to be PCI compliant with the majority of criteria.**

**Fact:** The pass mark for PCI is 100%, so if you fail even one of the criteria, you are not PCI compliant. The standard is not meant to be something to strive for; it is essentially a floor, a basis for further security measures. Failing to achieve even one of the requirements, is failing to meet a basic standard for handling cardholder information. All companies that routinely handle this type of data should be aiming to exceed the standard. It's just good business.

**Myth: I only need to protect my credit card data, not ATM debit card related data.**

**Fact:** Incorrect - both are required. Many debit cards are dual-purpose 'signature debit', which can be used on debit and credit card networks. As such, they are covered under PCI and must be protected in the same way as credit cards.

**Myth: I can wait until my business grows.**

**Fact:** Incorrect - the PCI standard applies to all sizes of business and waiting could be costly. Should you be compromised and not be PCI compliant, the fines and the compensation requirements by the banks (it typically costs between \$50 and \$90 to replace one card) could be substantial.

**Myth: I can just answer 'yes' to all the criteria on the Self-Assessment Questionnaire (SAQ).**

**Fact:** The Self-Assessment Questionnaire (SAQ) is a mechanism for getting the information about the level of your compliance to your merchant bank. The

standard applies at all times. Just saying yes to the questions puts you at great risk. If a compromise took place and it was obvious that you were not and have never been PCI compliant, the matter would be taken very seriously. You would be risking your whole business by answering 'yes' to the questions, when there is no factual basis for the answers.

**Myth: I can wait until my bank asks me to be PCI compliant.**

**Fact:** The dates for merchants to be PCI compliant are long gone. You are responsible for making sure you are in compliance. Waiting until the bank asks you could be very costly indeed.

**Myth: As a merchant, I did not sign anything saying I would be compliant; therefore, I don't need to be.**

**Fact:** The PCI standard forms part of the operating regulations that are the rules under which merchants are allowed to operate merchant accounts. The regulations signed when you open an account at the bank state that the VISA regulations have to be adhered to. Even if you have been in business for decades, PCI still applies if you store, process or transmit credit cards.

**Myth: As a merchant, I'm entitled to store any data.**

**Fact:** Many merchants believe that they own the customer and have a right to store all the data about that customer in order to help their business. Not only is this incorrect regarding PCI, it may also be a violation of State and Federal legislation regarding privacy. The PCI regulations specifically forbid storing of any of the following:

1. Unencrypted credit card number
2. CVV or CVV2
3. Pin blocks
4. PIN numbers
5. Track 1 or 2 data

Any of the above found in databases, log files, audit trails, backup's etc. can result in serious consequences for the merchant, especially if a compromise has taken place.

**Myth: One vendor and product will make us compliant.**

**Fact:** Many vendors offer an array of software and services for PCI compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI DSS. When marketing focuses on one product's capabilities and excludes positioning these with other requirements of PCI DSS, the resulting perception of a 'silver bullet' might lead some to believe that the point product provides 'compliance', when it's really implementing just one or a few pieces of the standard. The PCI Security Standards Council urges merchants and processors to avoid focusing on point products for PCI security and compliance. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the 'big picture' related to the intent of PCI DSS requirements.

**Myth: Outsourcing card processing makes us compliant.**

**Fact:** Outsourcing simplifies payment card processing but does not provide automatic compliance. Don't forget to address policies and procedures for cardholder transactions and data processing. Your business must protect cardholder data when you receive it, and process charge backs and refunds. You must also ensure that providers' applications and card payment terminals comply with respective PCI standards and do not store sensitive cardholder data. You should request a certificate of compliance annually from providers.

**Myth: PCI compliance is an IT project.**

**Fact:** The IT staff implements technical and operational aspects of PCI-related systems, but compliance to the payment brand's programs is much more than a 'project' with a beginning and end – it's an ongoing process of assessment, remediation and reporting. PCI compliance is a business issue that is best addressed by a multi-disciplinary team. The risks of compromise are financial and reputational, so they affect the whole organization. Be sure your business addresses policies and procedures as they apply to the entire card payment acceptance and processing workflow.

**Myth: PCI will make us secure.**

**Fact:** Successful completion of a system scan or assessment for PCI is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

**Myth: PCI is unreasonable; it requires too much.**

**Fact:** Most aspects of the PCI DSS are already a common best practice for security. The standard also permits the option using compensating controls to meet some requirements. The standard provides significant detail, which benefits merchants and processors by not leaving them to wonder, 'Where do I go from here?' This scope and flexibility leads some to view PCI DSS as an effective standard for securing all sensitive information.

**Myth: PCI requires us to hire a Qualified Security Assessor (QSA).**

**Fact:** Because most large merchants have complex IT environments, many hire a QSA to glean their specialized value for on-site security assessments required by PCI DSS. The QSA also makes it easier to develop and get approval for a compensating control. However, PCI DSS provides the option of doing an internal assessment with an officer sign-off if your acquirer and/or merchant bank agrees. Mid-sized and smaller merchants may use the Self-Assessment Questionnaire (SAQ) found on the PCI SSC Website to assess themselves.

**Myth: PCI makes us store cardholder data.**

**Fact:** Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card. If merchants or processors have a business reason to store front-card information, such as name and account number, PCI DSS requires this data to be encrypted or made otherwise unreadable.

**Myth: PCI is too hard.**

**Fact:** Understanding and implementing the 12 requirements of PCI DSS can seem daunting, especially for merchants without security or a large IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyways to protect sensitive data and continuity of operations. There are many products and services available to help meet the requirements for security – and PCI compliance.

When people say PCI is too hard, many really mean to say compliance is not cheap. The business risks and ultimate costs of non-compliance, however, can vastly exceed implementing PCI DSS – such as fines, legal fees, decreases in stock equity, and especially lost business. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your ongoing business plan and budget.