

Frequently Asked Questions

Q: What is PCI DSS compliance?

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 and protect cardholder data. The first set of data security requirements was created by Visa in 2000. The Payment Card Industry Security Standards Council (PCI SSC) was created in September 2006 to manage the ongoing evolution of the data security standards. The PCI DSS is administered and managed by the PCI SSC, an independent body created by the major payment card brands. Compliance is **mandatory** for any merchant or other organization that accepts payment cards. The PCI DSS can be found at www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

Q: Who enforces PCI compliance?

The payment card brands, such as Visa, MasterCard and American Express, and acquiring banks, such as Wells Fargo, First Data and others, are responsible for enforcing that your restaurant is in compliance with the Payment Card Industry Data Security Standard.

Q: What are the PCI compliance deadlines?

All deadline enforcement will come directly from your merchant bank or payment card brands. [Click here](#) for more information on data security deadlines.

Q: What does my restaurant have to do to be compliant with data security standards?

The requirements for being compliant with data security standards all revolve around one primary goal – protecting cardholder data – and include both security technology and security process-related instructions. Many restaurant operators falsely believe that having a validated payment processing application equals PCI compliance. Demonstrating PCI compliance goes well beyond this. You are directly responsible for ensuring that your restaurant meets **ALL** requirements of the PCI DSS standard and for reporting your compliance status. To prove compliance, at the very least, you are required to complete the PCI Self-Assessment Questionnaire (SAQ) on an annual basis and engage an Approved Scanning Vendor (ASV) to perform quarterly security scans on your infrastructure.

Q: How long have these requirements been in place and how do I find out which companies offer products validated against the Payment Application Data Security Standard?

The first set of requirements for payment applications were introduced in April 1, 2000 by Visa and were commonly known as the Cardholder Information Security Program (CISP). In 2004, Aloha POS was the first restaurant POS product to be certified against the CISP requirements. Since then, various other restaurant POS system vendors have also had their applications validated and a list can be found at https://www.pcisecuritystandards.org/security_standards/vpa/.

Q: My bank and payment processors have started sending me letters saying that I have to be using a Payment Application Data Security Standard (PA-DSS) compliant version of my POS software by July 1, 2010. What does this mean and why are they sending me all these letters?

As of July 1, 2010, Visa has mandated that all businesses that process, store or transmit card data must be using a payment application validated against the payment application data security standard (PA DSS). Your acquiring bank must provide periodic reports to Visa verifying that you and all of its clients are running a validated payment application in your restaurant. If you cannot show your bank that you

are running a PA-DSS compliant version of POS software, they will report to Visa that you are not running a compliant versions and fines may be passed down.

Q: I received a letter from a 3rd party application provider that integrates with my POS solution. Do I have to upgrade that solution when I upgrade my POS solution to remain compliant?

Unless the 3rd party application is being passed sensitive data from your POS system, upgrading that application is not related to PCI compliance. You may have to upgrade, however, in order for the 3rd party app to continue working with your updated version of the POS application.

Q: What are the potential implications to my business if I am found not to be PCI compliant?

You are required to prove to your merchant bank that you are PCI compliant by completing the Self-Assessment Questionnaire and performing quarterly security scans. If Visa gets a report from your merchant bank stating that you have not shown your restaurant to be PCI compliant, they may fine your bank from \$5,000 to \$100,000 per month for these violations. Your bank will most likely pass part of these fines down to you. They may also increase your transaction fees or terminate your relationship with them.

Q: Does being PCI compliant mean that my business will be protected from cyber-crime/security breaches?

Compliance does not imply security. You are compliant with mandates and regulations only at a specific point in time. To be secure, you must ensure that you are running your business in a secure manner at all times. That means that you must continuously monitor your security processes, ensure you are implementing required patches to your OS and payment processing applications, and perform continuous security scans on your infrastructure perimeter.

Q: If my site were to be breached, what would be the business/financial implications to my business?

The fines, penalties and forensics costs of a data security breach are staggering. The payment card brands will assess you fines ranging from \$5,000 to over \$50,000. In addition, you must hire a Qualified Incident Response Assessor if your site security becomes compromised and these fees can range from \$10,000 - \$25,000. Ultimately, the cost of a data security breach can overwhelm your business, severely damage your reputation and in extreme cases put you out of business.