

PCI Frequently Asked Questions *continued*

How can I find out if I am at risk?

You can go to our free Risk Profiler at <http://chasepaymentech.riskprofiler.net> and answer a brief questionnaire to determine your risk of having customer credit card data stolen from your computers. There is no charge for Chase Paymentech merchant clients to go through the Risk Profiler. Simply visit <http://chasepaymentech.riskprofiler.net> and enter CPSPCI2008 to get started.

How can I validate compliance?

Chase Paymentech has arranged preferential pricing with Trustwave (www.trustwave.com). Trustwave's compliance solution is a simple, cost-effective method for validating compliance with the PCI DSS, for all the major payment brands' security programs. Simply go to <http://chasepaymentech.trustkeeper.net> and enter CPSPCI2008 in the Enrollment Code field.

Once I become compliant, how long am I considered compliant and what are the compliance deadlines?

All merchants are required to maintain compliance at all times. Please refer to the table in our Alert for current requirements by Merchant level. You may view the Alert and the chart at: <http://www.chasepaymentech.com/pcialert>.

For more information about how you can ensure your PCI compliance, please contact your Chase Paymentech representative.

CHASE ™
Paymentech

CARDHOLDER DATA SECURITY Compliance Requirements



Avoiding risk and seeking compliance — your guide to understanding your responsibility under the Payment Card Industry Data Security Standards (PCI DSS).

CHASE ™
Paymentech

Your Responsibility, Security and Accountability

Providing customers a secure way to pay is more than just good business — it's a requirement. Fulfilling appropriate requirements helps merchants avoid security compromises for which they could be held liable. The fact is, non-compliance fines and related liability could cost you thousands of dollars. To help, the major payment brands established the Payment Card Industry Data Security Standards (PCI DSS) aligning Visa's CISP, MasterCard's SDP and other payment brands' cardholder data security program requirements. Chase Paymentech has created this guide to help you understand your responsibilities. For more detailed information, please see our Alert at <http://www.chasepaymentech.com/pcialert>.

PCI Frequently Asked Questions

Does PCI DSS apply to me?

Yes. It applies to all entities that store, transmit or process cardholder data regardless of whether payment is received online, by mail/telephone orders or face-to-face. It also applies to any network component, server or application included in, or connected to, your cardholder environment.



Why must I go through the compliance process?

There are several reasons for compliance. Below are just a few:

- Avoiding loss of your customers' trust and loyalty.
- Identifying and addressing your vulnerabilities.
- Protecting your customers' sensitive data.
- Fines from the payment brands can cost up to \$50,000 per month and/or egregious fines of up to \$500,000.

What is required to become PCI DSS compliant?

The Chase Paymentech Payment Brand Data Security information web page at <http://www.chasepaymentech.com/datasecurity> is your first stop in learning about requirements.

How do I know if my payment application is compliant?

Go to the Chase Paymentech Card Brand Data Security requirements page (listed above), and click on the link to Visa's CISP Tools & FAQ. Then view the CISP-Validated Payment Applications and Payment Applications Best Practices documents.

Is Chase Paymentech compliant?

Yes, and we will continue to be compliant with the PCI DSS. In 2007, we were named an inaugural member of the PCI Security Standard Council (PCI SSC) Board of Advisors.

continued on back