

Payment Card Industry (PCI) Data Security Standard (DSS)

Common Questions

Qualifying Questions

Does your client or any of their business units:

- accept credit cards as a form of payment?
- build software for the processing of credit cards?
- allow customers to swipe credit cards?
- accept payments online?
- process payments on behalf of others or involved in the processing of credit cards?

What is the Payment Card Industry (PCI) Data Security Standard (DSS)?

The PCI Data Security Standard represents a common set of industry tools and measurements to help ensure the safe handling of sensitive information. Initially created by aligning Visa's Account Information Security (AIS)/Cardholder Information Security (CISP) programs with MasterCard's Site Data Protection (SDP) program, the standard provides an actionable framework for developing a robust account data security process - including preventing, detecting and reacting to security incidents.

What are the deadlines for complying with PCI DSS?

Compliance is mandated by the payment card brands and not by the PCI Security Standards Council. However, for most merchants, the deadlines for validating compliance with the PCI DSS have already passed. You should check with your acquirer and/or merchant bank to check if any specific deadlines apply to you, based on merchant transaction volume (level) as determined by the card payment brands. **All entities that transmit, process or store payment card data must be compliant with PCI DSS.**

What are the penalties for non-compliance?

- Visa and the other payment brands reserve the right to fine acquiring banks for the non-compliance of their merchants
- Acquiring banks reserve the right to fine merchants for non-compliance.
- Fines are not set, but the following have been observed
 - \$10,000 per month for 12 months
 - \$25,000 for the 13th month
 - \$50,000 for the 14th month
 - +\$25,000 per month per month
- In the case of a breach, if the vendor is found to be out of compliance, damages can also be imposed to the vendor.

Payment Card Industry (PCI) Data Security Standard (DSS)

Common Questions

What is the definition of "merchant"?

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.

I'm a small merchant who has limited payment card transaction volume. Do I need to be compliant with PCI DSS? If so, what is the deadline?

All merchants, whether 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.

Does PCI DSS apply to debit cards, debit payments, and debit systems?

Any payment card (credit, debit, prepaid, stored value, gift or chip) bearing the logo of one of the PCI Security Standards Council's five founding payment brands is required to be protected as prescribed by the PCI DSS.

Does PCI DSS apply to merchants who use payment gateways to process transactions on their behalf, and thus never store, process or transmit cardholder data?

PCI DSS requirements are applicable if a Primary Account Number (PAN) is stored, processed, or transmitted. If PAN is not stored, processed, or transmitted, PCI DSS requirements do not apply. However, under PCI DSS requirement 12.8, if the merchant shares cardholder data with a third party processor or service provider, the merchant must ensure that there is a contractual obligation for that third party processor/service provider to adhere to the PCI DSS and that the third party processor/service provider is responsible for the security of the cardholder data it possesses. In lieu of a direct agreement, the merchant must obtain evidence of the third-party processor/service provider's compliance with PCI DSS via other means, such as via a letter of attestation.

For more information contact Thomas Lewis at 615-309-2296; tlewis@lbmc.com.