

Payments



Merchant Protection Program

People do business with companies they trust; your brand and reputation depend on data security. Merchant Protection Program can help guide you through the process of validating and maintaining PCI DSS compliance.

Why is customer card data security important to merchants?

Your business depends on your reputation and integrity. Ensuring cardholder data is secure will allow you to continue to grow your business while maintaining the integrity of your reputation. A security incident at your merchant location could result in loss of sales, adverse reputational damage, and increased cost due to fines.

The PCI Data Security Standard (PCI DSS) was established in 2006 by the major card brands (Visa, MasterCard, American Express, Discover Financial Services, and JCB International). All businesses that process, store, or transmit payment card data are required to comply with the PCI DSS.

What is PCI DSS—Payment Card Industry Data Security Standard?

The PCI DSS represents a common set of industry tools and measurements designed to ensure the safe handling of cardholder information. The standard provides an actionable framework for developing and maintaining data security, including the prevention, detection, and response to security incidents. If your business accepts card payments, PCI DSS compliance is required by card brands.

For additional information, visit the Payment Card Industry Security Standards Council's (PCI SSC) website.

Heartland Merchant Protection Program

Heartland is pleased to announce a new partnership for U.S. merchants with ControlScan, a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). To demonstrate our level of commitment to our merchants, we have partnered with ControlScan to develop our Merchant Protection Program, a small business program that provides our merchants with the resources needed to achieve and maintain PCI DSS compliance validation.

Who can benefit from the Merchant Protection Program?

The Merchant Protection Program applies to all Level 4 Merchants, though all merchants are required to be PCI DSS compliant. Level 4 Merchants are all merchants processing less than 20,000 eCommerce transactions per year, per card brand and all other merchants - regardless of acceptance channels—processing up to 1 million transactions per year, per card brand.

What are the benefits of the Merchant Protection Program?

- Merchants can achieve and maintain compliance validation to the PCI DSS, as required by the card brands. PCI DSS compliance is not a single event, but an ongoing process. As technology and card processing situations change, the Merchant Protection Program is designed to help you manage, assess, and demonstrate compliance efforts around data security.
- ControlScan assists merchants in validating compliance through an online portal where you can access the intuitive, easy-to-understand SAO, vulnerability scans, and live support.
- Merchants can receive the education and necessary guidance relevant to the Payment Application Data Security Standard (PA DSS) and the new Visa Mandate associated with Qualified Integrated Resellers (QIR).
- Merchants can reduce the likelihood of possible fines imposed by the card brands by using the tools designed to ensure that business policies and practices meet the PCI DSS.
- Merchants will benefit from quarterly IP scans that review systems for common vulnerabilities targeted by hackers and receive information regarding remediation strategies.

Merchants will be eligible for forgiveness of card brand fines imposed in the event of a breach, up to \$100,000, subject to program limitations.

What is a Qualified Integrator and Reseller (QIR)?

A Qualified Integrator and Reseller (QIR) is an organization qualified by the PCI SSC to implement, configure and/or support PA DSS validated Payment Applications on behalf of merchants and service providers. The quality, reliability and consistency of a QIR's work provide confidence that the application has been implemented in a manner that supports the merchant's PCI DSS compliance.

How do I get started?

Merchants are automatically enrolled into the Merchant Protection Program. When you are ready to activate your use of the Merchant Protection Program, please have the following information available:

- Enrollment information provided by Heartland.
- All external facing IP Address/es where card data is stored, processed or transmitted.
- Details of third party partners associated with your processing environment, if any
- Authority to proceed (from the business owner if it's not you)

Contact ControlScan at 800.477.3590 to get started. Choose Option #1 for support.

Am I required to use ControlScan?

The Merchant Protection Program makes it easy for you to complete PCI DSS validation. Although we recommend that merchants use ControlScan, you may provide proof of your current validation of compliance from another vendor.

