Bank of Hawaii

Merchant Services

Q&A: Complying, and validating compliance, with the Payment Card Industry Data Security Standards

QUESTION	ANSWER
Q. Why am I being contacted?	➔ A. In order to prevent the rise in cardholder fraud and identity theft, the Payment Card Industry Security Standards Council – founded by Visa®, MasterCard®, and other major payment card companies – has developed and implemented a single comprehensive PCI Data Security Standard (PCI DSS). All organizations that accept payment cards must comply with these standards to continue to process payment card transactions. The purpose of contacting you by surface mail, email, or telephone is to advise you to participate in SecurityMetrics' Site Certification Program. The Site Certification Program offered by SecurityMetrics, along with Bank of Hawaii's validation requirements for all merchants, ensures your organization's compliance with the risk vulnerability program known as the Payment Card Industry Data Security Standard (PCI DSS). If you receive an email, your organization has an internet presence and your email address is listed as the contact. SecurityMetrics, Inc. is a Qualified Security Assessor and Approved Scanning Vendor.
Q. What does the Site Certification Program do?	➔ A. Site Certification includes a self-assessment questionnaire and a computer network scan, as applicable, to determine compliance with PCI DSS. A single SecurityMetrics Site Certification test is accepted by Visa®, MasterCard®, Discover®, American Express®, Diners®, and JCB®. Validating compliance with the PCI DSS Requirements will indemnify you from fines and penalties should cardholder data be stolen from your organization.
Q. How long does it take, what do I need to know, and is there a cost?	➔ A. Enrollment and testing is easy. On-line enrollment takes less than 10-minutes. Simply enroll and the service is scheduled to run at your convenience. Site Certification does not require any software installation, software configuration, training, or maintenance. Technical support is included. There are no additional fees charged by SecurityMetrics for Site Certification services (i.e., computer network scan and self assessment questionnaire). Before enrolling, determine what "payment card processing" category best describes your organization's card acceptance practices: a) performs card-not-present card acceptance – telephone orders, mail orders, and eCommerce or b) uses standalone dial up or internet enabled terminals or c) uses an integrated point-of-sale (POS) system – credit card equipment that is integrated with other office equipment in an office that may or may not have internet access and site to site communication. Be familiar with your organization's card-acceptance and back office computer usage and any computer services supplied by vendors. Be prepared to provide a list of all internet-facing IP addresses. If an integrated POS system is used, know the payment application product name, version number, and the payment gateway company, if any. If your organization has a website, know who the hosting company is. If it's an eCommerce website, know what functions the hosting company performs — security, data back up, etc — and the name of the "shopping cart" service provider.

QUESTION	ANSWER
Q. What if my organization doesn't have a website, use email, or use our computers for the internet?	➔ A. Although no computer equipment with internet access may be in use, SecurityMetrics still needs to determine the type of point-of-purchase terminal used to process payment card transactions. In this situation, if the terminal is not internet reliant then Site Certification may be minimal. Only SecurityMetrics can evaluate your particular situation regarding computer usage and determine your organization's level of validation that is required.
Q. What if I have a website, may be do a little eCommerce or none at all, but my organization has outsourced everything to a third party service provider?	➔ A. Many organizations feel that by using a third party service provider they are exempt from PCI DSS. Visa's position is the merchant's use of a third party service provider, gateway, hosting company, etc does not remove the organization from the responsibility to be compliant. This responsibility not only applies to preventing network intrusions but includes protecting retained copies of the transaction receipt as well.
Or, alternatively, what if my website is informational only?	Information only websites may also pose risks to your organization and your organization's customers. Hackers can take control of your organization's website and modify website links, or introduce new links, to take customers to phishing sites where personal information can be stolen. Any cardholder data stored on servers with externally-facing IP addresses can be stolen including cardholder data submitted by email.
Q. Whom do I call regarding questions about SecurityMetrics' Site Certification Program, costs to comply, and how my computer network is setup or other technical-related matters and its bearing on PCI DSS compliance?	➔ A. Questions regarding site certification testing and technical-related matters regarding your organization's computer network should be directed to SecurityMetrics at (801) 705-5665.
Q. Whom do I call regarding questions about my Bank of Hawaii Merchant Services account?	➔ A. Questions regarding your merchant services account and PCI DSS should be forwarded to either Merchant Service Customer Service at 694-7300 or Bob Gilfoy, Merchant Services Department, at 694-7309.
	Learn more about PCI DSS by going to: www.visa.com/cisp (Visa) www.mastercard.com/sdp (MasterCard) www.pcisecuritystandards.org (Payment Card Industry Security Standards Council)