bankonit

BY ROBERT D. GILFOY, ASSISTANT VICE PRESIDENT, MERCHANT SERVICES, BANK OF HAWAII

Protect yourself from credit-card fraud

It's a typical day at your office. Your inbox is full, your voicemail indicator is blinking rapidly and you just realized your 2 p.m. appointment has been moved to 9 a.m. — and it's now 9 a.m.!

Before running out to your appointment, your acquirer calls with bad news. Your business has been identified as a common point of purchase for fraudulent credit-card use crisscrossing North America. Fraud is being reported for purchases made in Baltimore, San Diego, Orlando and Seattle. The only thing the unhappy cardholders reporting the fraud have in common is: They're your customers! All have made credit-card purchases at your business during the past year.

It gets worse. You think you're the crime victim but, the way your acquirer sees it, you may be complicit in the theft of thousands of payment card numbers. Why? Your business is not registered as being compliant with the Payment Card Industry Data Security Standards (PCI DSS), a security standard to help organizations protect customer payment-card data. When you think it can't possibly get worse, your acquirer asks you, no, tells you, to put up a monetary reserve, and get this, the reserve amount is six figures, in order to pay for the forthcoming onslaught of industry fines and penalties.

It gets worse. You think you're the crime victim but the way your acquirer sees it, you may be complicit in the theft of thousands of payment card numbers.

Then you're provided a list from which to choose an industry-approved incident assessor who performs computer forensic investigations — a requirement for a suspected cardholder data breach — that adds another $20,000. You cry foul! You're just a small- to medium-size business that accepts payment cards.

What should you do to avoid this? First, accept that your organization must be PCI DSS compliant. Organizations that demonstrate and maintain PCI DSS compliance attain safe harbor from industry fines and penalties. Many organizations, although sincere, believe that PCI DSS does not apply to them. PCI DSS applies to all organizations that accept payment cards bearing the logos of American Express, Discover, JCB, MasterCard or Visa. The resistance to PCI DSS among small- to medium-size businesses in Hawaii, in my experience, lie in the confusion regarding how PCI DDS determines what actions are required by organizations to be PCI DSS compliant.

Actions include completing a self-assessment questionnaire (SAQ) and may include passing computer network scans administered by an Approved Scanning Vendor (ASV). Whether either or both actions are required and which questionnaire to complete will depend on how an organization processes card purchases.

The ways in which an organization processes card purchases are generally categorized as follows: a) performs card-not-present card acceptance telephone orders, mail orders and e-commerce; b) uses stand-alone dialup or internet-enabled terminals; or c) uses an integrated point-of-sale (POS) system credit-card equipment that is integrated with other office equipment which may or may not have internet access and site-to-site communication.

PCI DSS applies to all these categories. The categories determine which SAQ to complete and how the categories of card acceptance are segmented from Internet-facing IP addresses to determine if a computer network scan is required and what IP addresses are in scope. The good news: An ASV can quickly determine an organization's requirements.

Where do you start? Ask your acquirer for the name of the ASV it works with. Before calling an ASV, be prepared. Determine the payment card processing category that best describes your organization's card-acceptance practices. Be familiar with your organization's 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 payment gateway company, if any. If your organization has a Web site, know who the hosting company is and, if it's an e-commerce Web site, know what functions it performs — security, data back up, etc. — and the name of the "shopping cart" service provider. Once prepared, make a call to the ASV and determine your organization's PCI DSS requirements. You're now on your way to being PCI DSS compliant and attaining safe harbor.

Once done, ensuring a typical day at the office remains just that! SB