



Minding the (Small) Stores

Help small merchants scrap vulnerable payment software and limit the risk to your business

By Rick Allen

Anyone involved in the development or integration of software that stores, processes, or transmits payment-card transaction data for commercial products or internal systems knows that application security compliance is required of some but only recommended of others. Service providers, for example, have long been required to assess and demonstrate secure software developmental practices to successfully prove PCI compliance. Many commercial-product companies that develop stand-alone, deployed payment applications and point-of-sale (POS) systems, however, are not contractually obligated to become compliant and see payment application security as a recommended best practice. But in the past two years, several companies have *voluntarily* updated their application systems to adhere to Payment Application Best Practices (PABP) standards. Why? Because they understand that helping merchants become PCI-compliant makes good business sense for everyone.

Recent industry developments made payment application security compliance a standard requirement. With representation from major payment card brands, the PCI Security Standards Council recently adopted Visa's PABP as the Payment Application Data Security Standard (PADSS).

While everyone wants to feel secure as possible, ISOs, acquirers, and third-party agents don't like potentially intrusive regulations telling them how to get there. However, they need to understand that as a result of the action, companies are creating trusted, validated software, and the large number of small merchants can now become PCI-compliant more easily. Validated payment software is an important building block of trust in the payment system. Making application security a requirement best positions compliance as an achievable standard that can be embraced by many, instead of a marketing tool offered by a few.

What's in It for You

Many important issues compete for your attention, so why should you care about payment application security? Simple, it supports your objective to protect your customer's best interests by making it easier for that customer to become PCI-compliant. The security and compliance of payment applications are critical issues for ISO agents and processors who hold liability for merchants. The risks to your business and reputation increase with the number of merchants who use vul-

The security and compliance of payment applications are critical issues for ISO agents and processors who hold liability for merchants. The risks to your business and reputation increase with the number of merchants who use vulnerable payment software applications.

nerable payment software applications.

Most industry experts agree that one of the largest threats to the payment system is vulnerable payment applications, which have proved to be the leading cause of compromised data incidents, particularly among small merchants. When asked if they store credit card data on the merchant application and



agreement, your customers probably do not understand the question or how the wrong answer may prevent them from becoming PCI-compliant. A compulsory validation of payment applications, however, creates a sustainable and secure environment. In addition, you can have the confidence of knowing that the current version of your payment software application does not store sensitive account information; provides proper encryption security controls needed to protect account information and prevent a data

compromise; and is installed and operated to support PCI compliance at the merchant location.

Many merchants believe that the software company is responsible for protecting cardholder data that is transmitted, stored, and processed in the system. This is especially true of merchants using commercial, off-the-shelf systems that don't require customized features. Even as payment application has moved from a recommendation to a requirement, no stakeholder is responsible for enforcing software vendors to comply with PCI and payment application security standards. How can industry and market forces combine to create an environment that compels more vendors to build compliant software and validate? Remember, it's the vendor customers (who hold merchant agreements) with acquiring banks that must be PCI-compliant.

In October (shortly after the PCI Security Standards Council adopted the former PABP as the new PADSS), Visa USA quietly announced new security mandates to eliminate the risk of nonsecure payment applications from the Visa payment system. Over the next three years, these mandates will force acquirers and agents to ensure that merchants are using payment software that adheres to payment application security standards. Many acquirers, however, had already started to require that only validated or compliant payment applications be certified to their systems before the new mandates were announced. By establishing the basis for accountability, acquirer compliance efforts are reinforced and merchants cannot switch processors to avoid meeting security requirements.

How to Help

Payment application security compliance and validation can be a barrier or a bridge, depending on your viewpoint. Here are some practical tips and advice on how to make the best of the situation and turn security barriers into bridges for new opportunities to increase market share and your base of satisfied merchants who remain loyal to your brand and thrive in a secure payments infrastructure.

- **Know your risk tolerance.** Acquirers are required by payment-card brand operating regulations to ensure that their



Your role is to promote payment-application security by understanding that merchants who use applications with inherent security flaws are at a higher risk for data compromise.

agents and merchants comply with cardholder-information security programs. Your role is to promote payment-application security by understanding that merchants who use applications with inherent security flaws are at a higher risk for data compromise. With incidents on the rise, both you and your merchant will waste time, money, and more importantly, your established goodwill when a security incident occurs. Merchants complain about software vendors using PCI security

to sell software upgrades that include new features that customers don't need. The business case to upgrade is justified, however, if the new software provides a compliant, validated payment application.

- **Help your partners and customers understand the critical nature of the issue.** The first of five payment-application security mandates went into effect on January 1. This phase deters vendors from introducing vulnerable software into the payment system by prohibiting acquirers from boarding new merchants who use known vulnerable applications. If your customers are using outdated non-compliant software, they won't be able to process transactions unless they use compliant payment software that's validated. In other words: Don't sell old software to new customers when a validated software version is available.

The second phase begins July 1 and stipulates that only validated payment software applications can be certified to acquirer platforms. Now is the time to start promoting the business case with your software vendor for building compliant payment software and getting validated before starting or completing integration with an existing platform.

- **Support small-merchant PCI compliance.** Many acquirers, processors, and agents are beginning to use standardized profiling methods to identify and ensure that high-risk merchants undertake the most appropriate compliance action. The high-risk merchant profile includes those that always use high-speed Internet connections for transaction processing. Beginning October 1, acquirers must ensure that new level-three and level-four merchants are PCI-compliant. Using validated payment applications is a big part of doing that.

The vast majority of smaller merchants are concerned with building their business—not wrestling technology. The case has never been stronger for ISOs, processors, and agents to make payment application security of merchant software a key business enabler. **TT**



Rick Allen, CISSP, is the director of compliance for Payment Processing Inc. Reach him at rallen@paypros.com.