

PCI Compliance And Payment Applications: Facts And Myths

While there are many misperceptions surrounding PCI (payment card industry) compliance, the facts you need to know are relatively clear.

BY TRACY METZGER

One of the largest challenges for software developers in today's market is how to accept payments and manage PCI PA-DSS (Payment Application Data Security Standard) compliance. PCI compliance for payment applications is an industry requirement and merchant service providers (or payment processors) are required to cross-reference each newly boarded merchant's POS software to the approved list of compliant payment applications. This poses a serious problem for ISVs (independent software vendors) that have not taken their applications through the PA-DSS process and been certified as compliant.

Software development companies that have not engaged in the compliance process operate in fear of being left behind and frequently look for any "work-around" solution they can find or someone who will tell them that they don't need to be compliant. Unfortunately, there are no work-arounds for PA-DSS compliance. The bottom line is clear: If cardholder data passes through your application, then it requires PA-DSS certification, either encrypted or unencrypted.

Still, some ISVs are being told by certain resellers of merchant services that if they plug in a piece of middleware they are not required to have their software go through a compliance audit. In most cases, this middleware has passed its own PA-DSS audit and is listed as "validated," but just plugging middleware into an ISV's application doesn't necessarily make an ISV's application compliant. Other ISVs are being led to believe that implementing a point-to-point encryption solution into their software will make them compliant, but this is also not quite true. If you take this path and your application does not support other methods of swiping cardholder data, encryption will help reduce the scope of your audit but it still will not allow the application to fully meet current compliance standards.

There are also scenarios where the ISV uses encryption for cardholder data that passes through its application, then passes it to a middleware application, and then on to the processor. But since the data is still passing through your application and still needs validation, this does not take your application out of the scope of a PA-DSS audit.

That said, there are middleware solutions in the market today that can "outsource" the payments complete-

ly away from the ISV's solution and take over all aspects of the payment. But implementation of this type of solution requires a full understanding of what needs to be done from the ISV. Specifically, the steps to reach compliance through this approach include:

First, the ISV needs to embrace this solution completely. This means that there are no other payment solutions available within its application that can be used in lieu of the outsourced solution. Second, all peripherals that interact with the cardholder data need to be controlled by the middleware application. Third, any key-entered cardholder data needs to be entered only into the middleware application and not

passed from the ISV's application to the middleware application. Finally, the middleware application needs to be validated versus the PA-DSS standards and listed on the PCI website as a validated application. If you implement middleware without taking these four steps, your application will still be within the scope of a PA-DSS audit.

In the correct scenario, the middleware becomes the payment software, and, when the merchant services provider sets up the processing account, it registers the middleware as the payment software. Any other approach that does not take all aspects of the payment into consideration simply does not comply. These middleware products can be customized to look and feel like the ISV's application and even embedded into the install routine of the software, but they need to remain separate from a management and configuration standpoint.

The security of every transaction is critical to the payment industry, and following all of these steps correctly can help ISVs maintain a secure, compliant solution for their customers. If you are being told differently by a provider, then ask it for a PCI-certified security assessor's opinion and have them put it in writing. But understand that even this will not protect your customers in the unfortunate event of a data breach. If your customer is breached and your application is found to be out of compliance, there will be fines. They will be considerable, and they will certainly be directed at your customers regardless of any misunderstanding over what is or is not meant by PCI compliance. ●



TRACY METZGER

*Tracy Metzger
is the president of
T-Gate Payments.*



TGATE