

# Take The POS Out Of The Scope Of PCI

Contributed by Brad Adams, Director of Product Management, ISD Corporation, Inc.

Stop me if you've heard this one: a PCI auditor tells this retail merchant who has an aging POS application that he has until July 2010 to get all his payment related applications PCI compliant. That's it, no punch line, just reality.

Most merchants are painfully aware of the burden placed upon them by PCI, and they're not laughing. Not being PCI compliant in 2010 has serious consequences in the form of financial penalties and the looming threat of losing their ability to connect to acquiring bank processors necessary for getting non-cash payments authorized. 81% of merchants store payment card numbers somewhere in their system.

By July 2010, Acquirers must ensure their merchants, VisaNet Processors, and Agents use only PA-DSS compliant applications. Failure by merchants to comply and pass their PCI audits can result in those merchants being unable to connect to these acquirers and processors.

## The Merchant's Dilemma

As we find ourselves half way through 2009, many merchants still find themselves unprepared for their PCI audits by Qualified Security Assessors (QSAs) that may require them to spend large amounts of money in remediating their aging non-compliant POS payment applications. These merchants are also concerned about how little time remains before the July 2010 deadline arrives.

PCI was designed to make payment applications secure from cardholder data fraud. Some centralized payment application providers comply with the sections of PCI that apply directly to payment software vendors (known as PCI Payment Application Data Security Standards (PA-DSS)). "Having our ISD Payment Switch validated for PA-DSS is helping many merchants quickly prepare for next year, but it's just one piece of the entire puzzle," says Kevin Potrzeba, VP of Sales for ISD Corporation.

The POS applications in the stores are another piece of the payment processing transaction path that must comply with PCI if they handle sensitive card data. Whereas there are only a handful of centralized payment application providers in the industry, there are hundreds of home-grown and third party POS applications. It is safe to say that the majority of the POS applications haven't done enough to address PCI requirements.

There are literally thousands of articles posted to the web about the rampant spread of card data fraud happening around the world today. Criminals are highly motivated to move to the most vulnerable points in the payment transaction path to acquire the valuable card data. As the centralized payment switches become more secure, the ATM's and POS terminals, and their associated networks, become much more attractive as sources to steal card data. As a result, a huge percentage of these breaches are now occurring at the points where transactions originate, such as ATM's and POS terminals.

New stories of malware on in-store POS network lines and malicious applications inserted on unprotected and unsuspecting POS application servers are growing. NACSONline reports that 90% of all card breaches occur from such malware placed in the system. Having software on these servers that can detect the presence of unauthorized sniffers and rogue applications is critical to heading off a breach.

Not only do many of the POS applications lack the proper security detection software, many also lack the proper audit trails running on these servers to determine when, or to what extent, their systems have been breached.

This is very important to merchants because the capability to track the extent of the damage often plays a huge part in determining the amount of penalties and card reissuance costs a merchant will incur during the forensic phase of the breach. For example, if the merchant's POS application is incapable of determining the number of cards stolen, the PCI and Card Association representatives will attempt to determine that extent of the damage, and they will err on the side of caution; meaning they will assume the worst case scenarios to protect the largest number of card holders who may have been put at risk during the breach.

To summarize the points above, if they haven't already, thousands of merchants will soon become aware that their existing POS applications will not pass PCI requirements, and for the ones that do, these POS applications may still be insufficient to preemptively detect breaches or report the extent of the damage afterwards.

Thus, merchants are left with some painful choices. They can replace their POS applications at significant costs. Even if they have a budget and are willing to spend the money for PCI compliant solutions, many can't make such a radical change by July 2010; much less get the new POS applications PCI audited before then. Further complicating such an approach is that many POS applications are tightly integrated to other back office applications that depend on settlement information that might be compromised by such a radical change. Finally, if you are a merchant that wrote your own POS application, try and find the original programmers who would actually know how to make them PCI compliant.

#### Don't Change it, Insulate it

For merchants who do not see these choices as viable, there is another choice; simply take the POS out of scope of PCI. A common misconception about PCI is that it must be met across all applications in the payment transaction flow. In reality, PCI only applies to systems or network components that store, process or transmit cardholder data. PCI is binary on this point – 100% of PCI requirements apply to "in scope" systems and 0% of PCI requirements apply to "out of scope" systems. However, there is a trick to this. Networks containing in-scope systems must be logically isolated from networks containing out of scope systems.

Removing the flow of sensitive cardholder data from the POS is the quickest way to achieve this. There are logical boundaries that can be put around the POS application cost effectively that keep the POS from receiving any sensitive cardholder data.

One of the responsibilities of most POS applications today is to participate in the flow of sensitive cardholder data from the pin pads and magnetic stripe readers (MSR) to payment processors for authorization and settlement. From the moment a card is read, the coveted card account numbers and pins are in play and vulnerable to breaches. By removing the POS from this data flow and logically isolating the POS network from networks that transmit the sensitive data to processors, the POS is taken out of the scope of PCI. Since the POS never receives sensitive cardholder data and sits on a separate network, it is no longer in scope.

This does not mean that the POS cannot drive the payment process and store data related to the transaction – it absolutely can. It just means that the types of transaction data received by the POS don't include the full card number. Truncated card data (first six and last four digits) does not qualify as "Sensitive Cardholder Data" under the PCI requirements, but gives the retailer enough data to manage transactions.

This approach raises some challenges. The biggest is the construction of new payment applications and as well as alternate, secure store networks to carry the sensitive data. Until recently, conventional wisdom was that the cost of adding entirely new network segments and payment applications to the store environment would outweigh the benefit. However, new technologies such as virtualization of networks and hardware can be implemented alongside the merchant's existing infrastructure to provide this functionality at minimal cost.

Virtualization refers to implementing infrastructural components such as firewalls, routers, payment switches, and log servers as logically isolated instances of software running on a single physical piece of hardware instead of multiple devices. Since one of PCI's biggest criticisms is the requirement to implement and manage multiple expensive security gadgets, virtualization offers retailers low-cost alternatives. The homogeneity of retail systems across stores makes virtualized systems even more attractive, since the cost of system design can be amortized across multiple stores.

In a virtualized environment there are applications that can be rapidly put in place that provide new layers of security around the POS applications – without the need for new hardware or expensive software licenses. These applications not only cut off access to network and systems resources that hackers use to compromise payment systems, but can also detect those unauthorized sniffers and malicious applications before they have a chance to steal the card holders' data. These same solutions can also provide the audit tracking during a breach that often provide merchants with critical evidence that can be used to reinforce their innocents when suspected of a breach.

Note the emphasis that these three options can be added in parallel to the existing POS infrastructure, meaning they address the two pains originally addressed in the premise of this article: costly replacements and a lack of time to make these changes.

### Turning the Challenge into an Opportunity

Rather than replacing their POS infrastructure to meet the impending PCI deadlines, merchants have options that leverage their POS solution while insulating those investments with applications that draw the sensitive card data away from the POS and transport that data on more secured communications layers.

"Moving from legacy POS applications is an enormous challenge for merchants," says Mark Weiner, Managing Partner of Reliant Security which specializes in networking & security solutions that meet PCI requirements. "Not only do they need to address the costs of new hardware and software at their retail locations, but also the modification of complex backend systems and years worth of organizational investment in operating the platform. For businesses that are not ready to phase out their existing POS platforms, we have found that taking these systems out of PCI's scope is often the preferred alternative."

Finally, case studies show that the introduction of virtualized platforms in the retail store environment yields unique opportunities by providing a single platform to securely host new applications. Retail information technology did not stand still while PCI came along. There are a wide variety of innovative technologies that retailers can deploy to further managed their costs (inventory & IP telephony), maintain closer contact with their customers (email & CRM) and improved customer experience (pin-based debit & video on demand). Freed from the paradigm of buying hardware to support each new feature, retailers can not only meet PCI requirements, but support future development of their businesses.

[1] Forrester Consulting: The State of PCI compliance

[1] <http://www.nacsonline.com/NACS/News/Daily/Pages/ND0417098.aspx>