PCI COMPLIANCE

# Taking POS out of PCI Scope

*A PCI Solution White Paper by Reliant Security*


450 7th Avenue, Suite 503 • New York, NY 10123 • 917-338-2200
www.reliantsecurity.com

# Taking POS out of PCI Scope

*A Reliant Security White Paper*

## Overview

A common misconception among retailers is that PCI must be met across all applications associated with payment processing. In reality, PCI only applies to systems or network components that store, process or transmit cardholder data.

Traditionally, POS applications drive 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, card account numbers and pins are vulnerable to breaches. Removing the POS from this data flow and logically isolating the POS network from the other networks that transmit the sensitive data to payment processors can also have the effect of removing the POS from PCI's "scope," meaning that the POS itself is no longer subject to PCI requirements.

## The Merchant's Dilemma

One of the most challenging aspects of PCI compliance is addressing strict payment application security requirements mandated by the PCI council.

Criminals are highly motivated to move to the most vulnerable points in the payment transaction path to acquire the valuable card data. As centralized payment systems become more secure, POS terminals and their associated networks become much more attractive 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.

Many retail merchants have made significant investments in their POS applications and although aging, these applications remain critical to merchant businesses. Unfortunately, the credit card brands have directed acquirers and processors to decertify merchants that are not using validated payment applications, and potential financial penalties may also be assessed. Failure by merchants to comply and pass their PCI audits can result in those merchants being unable to submit transactions to these acquirers and processors.

Consequently merchants may still find themselves unprepared for an external PCI audit by Qualified Security Assessors (QSA's) that may require them to invest large sums of money to upgrade or replace their aging POS payment applications, in addition to other PCI-related infrastructure costs. Many POS applications lack proper security detection software and proper audit trails to determine when or to what extent their systems were breached. 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 estimate the extent of the damage and will:

- Err on the side of caution
- Assume the worst case in assigning liability
- Try and protect the largest possible number of cardholders who may have been put at risk.

As a result of these deficiencies, merchants are left with painful choices:

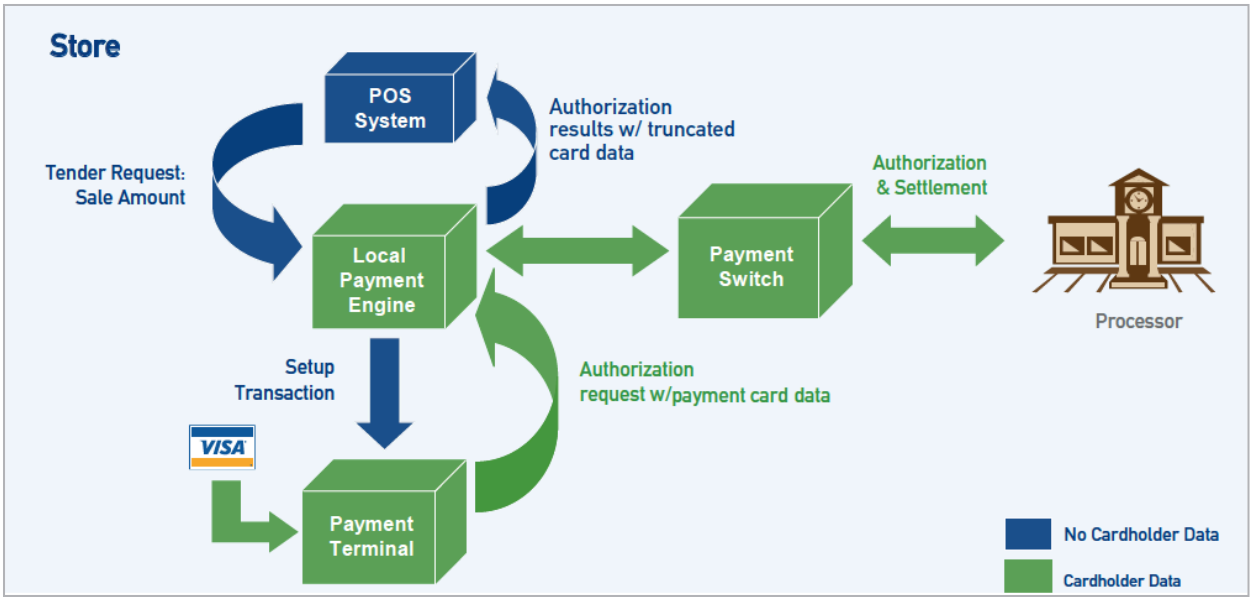
- They can replace their POS applications at a significant cost,
- Further complicating that approach is the fact that many POS applications are tightly integrated to other back office applications that depend on settlement information that might be compromised by such a radical change.
- Finally, merchants who wrote their own POS applications may have difficulty engaging the original programmers to make them PCI compliant.

### An Alternative Solution

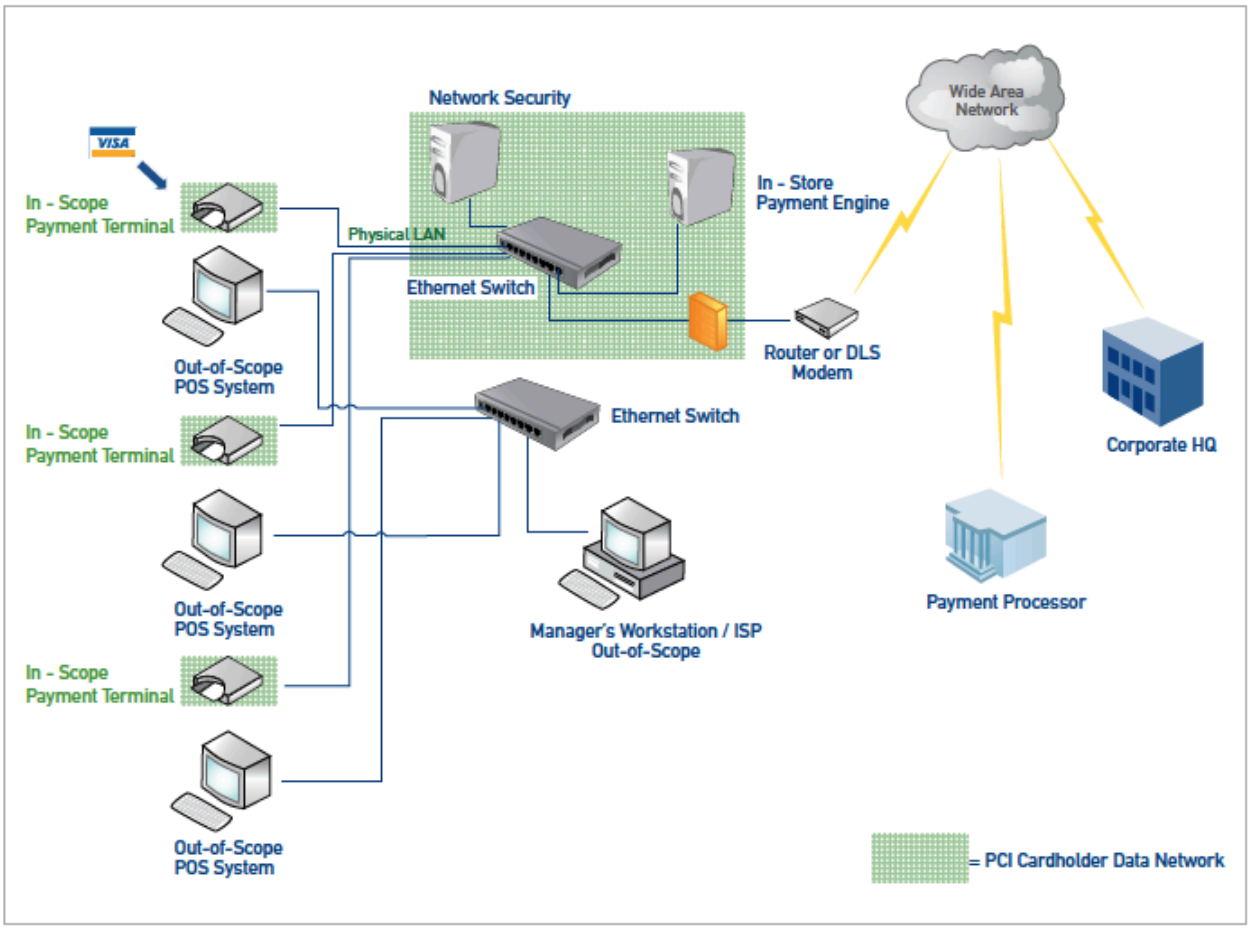
*The smart choice for a retail merchant is to take the POS out of the PCI scope.*

PCI applies to systems or network components that store, process or transmit cardholder data. It 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. Networks containing in-scope systems must be logically isolated from networks containing out of scope systems. In store systems, removing the flow of sensitive cardholder data from the POS is the quickest way to achieve this. Logical boundaries can be put around the POS application that keeps the POS from receiving sensitive cardholder data.

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) or tokens representing card data do not qualify as "Sensitive Cardholder Data" under the PCI requirements, but gives the retailer enough data to manage transactions.



PAYMENT TERMINALS AND PAYMENT ENGINE ON A SEGMENTED CARDHOLDER DATA NETWORK




Fortunately there is a class of payment software vendors and integrated POS vendors who provide functionality that conducts card transactions in a manner that is secure and that can be isolated from other store system components. This software was created to drive complex transactions on store PIN pads. PCI Auditors have evaluated such applications and validated that these applications can be used to completely offload payment-processing functionality from non-compliant POS applications.

In addition to the development of a new secure in-store payment engine, new secure store networks must be constructed to carry the sensitive data and host the PIN pads and payment engine. Until recently, conventional wisdom was that the cost of adding entirely new network segments and a new payment engine to the store environment could outweigh the benefit. However, new technologies such as virtualized networks and computer systems 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 engines, and log servers as logically isolated instances of software running on a single physical appliance instead of on multiple devices. One of the biggest criticisms of PCI is the requirement to implement and

manage multiple expensive security gadgets. Virtualization offers merchants a cost-effective and less complex alternative. The homogeneity of systems across stores makes virtualized systems even more attractive, as the cost of system design can be amortized across multiple stores.

Virtualization is widely recognized as a transformative technology that can be leveraged to reduce costs. In recognition of the technology's potential benefits, the PCI Standard Council published its virtualization guidelines in June 2011. Among other clarifications, this document provides guidance for hosting in-scope and out-of-scope systems on a single virtualized host. Additionally, the guidelines provide network segmentation requirements within virtualized systems.

Controls that provide new layers of security around the POS applications can be deployed rapidly without the need for new hardware or expensive software licenses. Virtual systems providing these controls cut off access to network and systems resources that hackers use to compromise payment systems, and can detect unauthorized sniffers and malicious applications before they have a chance to steal card data. These solutions can provide audit tracking during a breach to provide merchants with critical evidence to reinforce their innocence.

In summary, this architecture can be added in parallel to the existing POS infrastructure and can address two critical issues:

- Costly software and hardware replacements
- Lack of time to make these changes

## Turning the Challenge into an Opportunity

Rather than replace their POS infrastructure, merchants could instead move the sensitive card data away from the POS and transport it on more secure communication layers.

Migrating off legacy POS applications is an enormous challenge for merchants. For businesses not ready to take this step, we have experienced that taking these systems out of PCI scope is often the preferred alternative.

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 manage their costs (inventory & IP telephony), maintain closer contact with their customers (email & CRM) and improve their customer's experience (pin-based debit and digital signage). Freed from the paradigm of buying hardware to support each new feature, retailers can meet PCI requirements and support future development of their businesses.