

Merchant Security Checklist

(Updated: May 29th, 2008)

Note: This is not intended to be a complete PCI-compliance checklist. It is intended to cover the most critical, real-world aspects to securing the POS environment and protecting merchants. In the event of a compromise and subsequent security audit, the merchant will be checked for complete PCI compliance.

Color Code: **Vital** **Critical** **Urgent**

	Yes	No	Not Applicable
POS System			
The POS system doesn't store any Track data, CVV values, or PIN data.			
If the POS system stores account number and associated cardholder data, it's encrypted using an approved standard that meets requirements for strong cryptography (i.e. 2-Key TDES (2TDES), 3-Key TDES (3TDES), AES-128 or higher, RSA 1024-bit or higher, ElGamal 1024-bit or higher, Blowfish 128-bit or higher).			
The POS system deletes any stored card data after it's no longer needed, such as after a successful batch close.			
The POS system masks any card data contained in log files.			
The POS system logs employee activity.			
The POS system is kept up to date with vendor security patches.			
The POS system is PABP/PA-DSS compliant.			
POS Network			
The POS network is separated from the rest of the merchant's network.			
The POS network has a firewall protecting it from the internet and the rest of the merchant's network.			
All wireless devices on the POS network use WPA or WPA2.			
All wireless devices on the POS network are only used for POS connectivity.			
Wireless Access Points are configured so the administrative page can only be reached from a wired connection.			
Firewalls and routers are configured to have remote management disabled.			
Default passwords have been changed on all POS networking equipment.			
Merchant does not do web browsing, email, etc. on the POS system.			

	Yes	No	Not Applicable
Accessories			
All PIN Entry Devices are Visa or PCI PED Approved (See: https://www.pcisecuritystandards.org/pin/)			
Receipts are printed with card data masked on the customer copy (All but last four digits of card number masked, exp date masked).			
In TN, the merchant copy of the receipt is also masked. Soon, this will be mandatory in CA. It's highly recommended everywhere else.			
Merchant receipts with full card numbers are stored securely.			
Remote Access			
Remote access software is turned off by default and enabled temporarily when needed (Not necessary with LogMeIn).			
Remote access software is set up with unique logins for each user that accesses it.			
Remote access software is kept up to date with vendor patches.			
Software Management			
If Windows is used, the system has been updated to use Microsoft Update instead of Windows Update (See: http://update.microsoft.com). This will allow it to update other Microsoft products such as Office and SQL.			
If Windows is used, it's configured to install security patches automatically.			
Antivirus software is installed and updates automatically.			
Other software security patches are kept up to date (i.e. Mac OS, Linux).			
User Management			
Default user accounts have had their password changed from the default on all software, including the POS system and remote access software.			
Users have unique logins to the POS environment.			
Users change passwords at least every three months.			
User accounts are disabled or deleted after the employee leaves the company.			
All passwords are complex, consisting of at least eight characters and a mixture of character types (Upper case, lower case, symbols, numbers). This includes user passwords, remote access passwords, routers, firewalls, and wireless access points.			

	Yes	No	Not Applicable
Merchant Education			
The merchant is aware that they are liable for any lost or stolen card data.			
The merchant is on the lookout for suspicious employee activity such as writing down card numbers or skimming (Running cards through a device made for reading and storing card data).			
The merchant and their staff are aware of social engineering/con artistry and know to verify identities before allowing any access to the POS network.			
The merchant is on the lookout for rogue equipment such as unauthorized wireless devices plugged into the POS network.			
The merchant is aware that changes or service to the POS environment (i.e. systems, network equipment) should be approved by their dealer to ensure a secure environment is maintained.			
If the merchant has a web store, it is setup and maintained by someone that understands security and PCI.			
Merchant PCI Validation			
The PCI SAQ is filled out annually.			
An approved scanning vendor performs scans of the merchant network quarterly.			