

# MerchantResource



## Wireless Technology and Protecting Cardholder Data

### Wireless Convenience Demands Due Diligence

Wireless technology affords people many luxuries today, including garage door openers, TV remotes, cell phones, Wi-Fi Internet access and contactless payments. Because wireless equipment prices continue to decrease, more small- to medium-businesses are adopting the conveniences offered by wireless technology. Whether a coffee shop owner offers Internet access to customers, or a convenience store proprietor streamlines their inventory process, businesses are tapping into wireless technology now more than ever. But, these conveniences come with risks.

Research indicates that past high-profile payment card breaches were a result of the original breach occurring from the organizations' improperly configured wireless systems. Reports suggest that in many cases, thieves used a wardriving method – driving to various parking lots and using laptops, telescope antennae and wireless scanning software to scan or sniff for Wireless Access Points (WAP) that broadcast within the area. Because of the volume of stolen payment card numbers involved in these incidents, it's not likely that the thieves stole the card numbers over the wireless connection; however, the information the hackers needed to begin the security breach was collected through the organizations' wireless network.

### Secure Wired and Wireless Networks with PCI DSS Compliance

With the majority of payment card breaches investigated by AmbironTrustWave, the victimized organization did not comply with the Payment Card Industry Data Security Standard (PCI DSS) at the time of the incident. PCI DSS consists of 12 requirements and numerous sub-requirements aimed at securing the processing, transmission and storage of cardholder data on both wired and wireless networks. As mentioned above, a payment card compromise can start with the breach of a wireless network, but usually progresses with the exploitation of weak security elsewhere on the wired network. PCI DSS are based on industry-accepted security best practices that help organizations protect their networks from data security breaches.

### Getting Started

To help merchants better secure their networks and work toward PCI compliance, Chase Paymentech partnered with AmbironTrustWave, a compliance management and data security expert, to provide the expertise you need.

AmbironTrustWave works with thousands of merchants, from mom-and-pop shops to global operations, guiding them through the PCI DSS compliance process.

AmbironTrustWave's TrustKeeper® is an easy-to-use Web portal that helps merchants complete the PCI DSS Self-Assessment Questionnaire, schedule required scans, manage onsite audits and answer the questions they have about their network environment and PCI DSS compliance.

To get started, visit <http://www.chasepaymentech.trustkeeper.net>

If you have any questions, please contact AmbironTrustWave support at 1-888-878-7817.

## Wireless and PCI DSS: Considerations

While wireless technology continues to develop and increase in utility, wireless security is still maturing; therefore, data security experts caution that all wireless networks should be considered vulnerable to attack.

If an organization chooses to use wireless technology, we recommend they use it only for non-sensitive data transmission that is completely separate from the payment card processing, transmission or storage environments. Complete separation includes not only network segmentation or virtual LANs, but also strong access controls such as firewalls with policies that prevent any access to the payment card environment via the wireless network. PCI DSS require organizations to implement a firewall between any wireless network and the payment card environment to eliminate network traffic that is not absolutely necessary for business operations.

A common mistake in configuring wireless technology is failing to change the default settings on a device. In fact, hackers share lists of default settings for a number of available wireless products on Internet message boards. With that information, any unauthorized individual can compromise a wireless device not properly configured.

PCI DSS mandate that vendor default information be changed in regards to wireless environments and devices, such as:

- WEP (Wired Equivalency Protocol) keys
- SSID (Service Set Identifier)
- SSID broadcast be disabled
- SNMP (Simple Network Management Protocol) community strings on access points
- Vendor default login credentials
- WPA or WPA2 (Wi-Fi Protected Access) be enabled if device is capable\*  
*\*An organization evaluating wireless technology solutions should avoid any products not WPA capable. WEP alone has proven insufficient in protecting wireless communication and PCI DSS do not allow the use of only WEP.*
- Any other default settings

Wireless-Specific PCI DSS Requirements** (For entire standards list, visit <a href="http://www.pcisecuritystandard.org">www.pcisecuritystandard.org</a> .)						
1.1.2	2.2	2.3	8.5.1	10.3	10.5	12.3
1.3	2.2.1	3.4	8.5.15	10.3.1	10.5.1	12.3.1
1.3.8	2.2.2	4.1.1	9.1.3	10.3.2	10.5.2	12.3.2
2.1	2.2.3	6.1	10.1	10.3.3	10.5.3	12.3.3
2.1.1	2.2.4	8.4		10.3.4	10.5.4	12.3.4
				10.3.5	11.1	12.3.5
				10.3.6		12.3.6
						12.3.7

\*\*List of requirements should not be considered exhaustive. This list only includes PCI-DSS requirements that specifically mention wireless technology. Other PCI DSS requirements may also apply to the deployment of wireless technology, even if it is not listed above.

Remember, adhering to the above recommendations will not make your organization PCI DSS compliant, nor will it completely secure your wireless technology. The guidelines within this document serve as general considerations to help you achieve a more secure wireless technology environment.