



## CISP BULLETIN

# Use of Wireless Technology Requires Adequate Data Security Controls

August 29, 2006

---

Merchants that have implemented or are considering using wireless technology must develop and deploy a comprehensive strategy to secure their systems from intrusion. This includes any environment where cardholder information is being acquired, accessed, processed or stored. This article summarizes vulnerabilities that may occur in a wireless environment and provides recommended security controls to minimize the risk of a data compromise.

### The Importance of Wireless Security

The adoption of wireless technology is on the rise among participants in the payment industry — particularly retailers, many of whom use wireless technology for inventory systems or check-out efficiency (e.g., “line busting,” ringing up customers while they are in line). Because wireless technologies have unique vulnerabilities, all users must carefully evaluate the need for the technology and understand the risks, as well as the security requirements, before deploying wireless systems.

Wireless networks should always be considered “untrusted,” and Visa highly recommends that security controls be implemented on all such networks, regardless of their purpose. Nevertheless, if wireless technology is used to transmit cardholder data or if a wireless LAN is connected to or part of the cardholder environment (e.g., not separated by a firewall), wireless security features must be implemented.

It has come to Visa’s attention that some entities are not properly securing their wireless networks, which increasingly leads to the compromise of cardholder data, brand damage, and other concerns — both financial and regulatory. This risk is compounded when the entity stores full magnetic-stripe track data, Card Verification Value 2 (CVV2) or PIN blocks, all of which are prohibited by the PCI Data Security Standard and PCI PIN Security Requirements.

### Common Wireless Vulnerabilities

Following are some common methods of attacking wireless networks. These are widely documented on the Internet, complete with downloadable software and instructions.

- Eavesdropping — An attacker can gain access to a wireless network just by “listening” to traffic. Radio transmissions can be freely and easily intercepted by nearby devices or laptops. The sender or intended receiver has no means of knowing whether the transmission has been intercepted.



- Rogue Access — If a wireless LAN is part of an enterprise network, a compromise of the LAN may lead to the compromise of the enterprise network. An attacker with a rogue access point can fool a mobile station into authenticating with the rogue access point, thereby gaining access to the mobile station. This is known as a “trust problem,” and the only protection against it is an efficient access-authentication mechanism.
- Denial of Service (DOS) — Due to the nature of radio transmission, wireless LANs are vulnerable to denial-of-service attacks and radio interference. Such attacks can be used to disrupt business operations or to gather additional information for use in initiating another type of attack.
- Man-in-the-middle — Packet spoofing and impersonation, whereby traffic is intercepted midstream then redirected by an unauthorized individual for malicious purposes, are also valid threats.

### Wireless Security Strategy

Entities that have implemented or are considering implementing wireless technology should develop and implement a comprehensive strategy to secure the environment. Acquirers must ensure that their merchants using wireless:

- Have a proper awareness of the security risks associated with the technology
- Develop risk-mitigation strategies to protect their computing environments — compliant with the Cardholder Information Security Program, PCI PIN Security Requirements and the PCI Data Security Standard
- Evaluate all payment applications against the *Payment Application Best Practices* posted on [www.visa.com/cisp](http://www.visa.com/cisp) to ensure full magnetic-stripe track data, CVV2 or PIN blocks are not stored or logged subsequent to the transaction

Following are wireless security precautions to implement in conjunction with the corresponding PCI Data Security Standard requirement. Members are encouraged to share these important security practices with their merchants and agents. Members are responsible for ensuring their merchants and agents promptly correct any security vulnerabilities.

<b>Wireless Security Precaution</b>	<b>Related PCI Data Security Standard Requirement</b>
Utilize network segmentation to protect assets. The credit card processing environment must be segmented from public networks, including wireless networks, so that in the event of a network problem, the issue is isolated to the affected subnet. Advantages of network segmentation include, but not limited to: <ul style="list-style-type: none"><li>• Increased network performance</li><li>• Effective bandwidth utilization</li><li>• Physical separation of network traffic of different security levels</li></ul>	1.3
Implement strong Access Control List (ACL) router rules. ACLs will help to block traffic on known ports, which should not be present on the protected network.	1.3

Wireless Security Precaution	Related PCI Data Security Standard Requirement
Check your AP router/firewall to ensure it is not configured to allow PING requests from the Wide Area Network (WAN)	1.3.5
<p>Always change the vendor-supplied defaults, as follows:</p> <ul style="list-style-type: none"> <li>• Change default passwords. Default passwords for popular wireless devices are well known to hackers and often available on the Internet.</li> <li>• Change default Service Set Identifier (SSID) on the wireless access point (AP). An SSID can be sniffed in plain text from a packet and does not supply any security. SSID character strings should not reflect a name or company identifier.</li> <li>• Disable SSID broadcast.</li> </ul>	2.1.1
Disable all insecure and nonessential protocols on the wireless AP.	2.2.2
Management of the APs must be performed from within the network. Enable two-factor authentication for the management interfaces of wireless APs and use SSL/TLS for Web-based management.	2.3 and 8.3
<p>Implement Wi-Fi Protect Access (WPA) or WPA2 to encrypt transmissions. Never rely on Wired Equivalency Privacy (WEP), which has well publicized vulnerabilities. WPA or WPA2 provides a stronger alternative to WEP. The primary difference between WPA and WPA2 is that WPA2 uses a more advanced encryption called AES (Advanced Encryption Standard).</p> <p>WPA or WPA2 operate strictly between your Wi-Fi device and wireless AP. When data reaches the AP, the data is unencrypted and unprotected so VPN technologies or SSL/TLS must be used to protect transmission from public networks.</p>	4.1.1
Keep security patches on the wireless APs up to date.	6.1
Make sure reset functions on the wireless APs are used only when needed and can only be invoked by authorized individuals.	7.1
<p>Access to a wireless network should be granted based on a wireless client's identity. Authentication systems should examine a client's identity and grant or deny access. When implementing WPA or WPA2, organizations should choose Enterprise mode instead of Personal, or Pre-Shared Key (PSK), mode.</p> <p>PSK mode:</p> <ul style="list-style-type: none"> <li>- Does not require an authentication server</li> <li>- Does require a strong "shared secret" key that is used for authentication of devices but is not used for encryption</li> </ul> <p>Enterprise mode:</p> <ul style="list-style-type: none"> <li>- Requires the existence of an authentication server</li> <li>- Protects the log-on process using the RADIUS protocol</li> <li>- Offers centralized user management for the wireless network</li> </ul> <p>Enterprise mode is more secure than PSK and adds the benefit of scalability for larger wireless networks. PSK can be strong and reliable based on the complexity and length of the key, but updating keys throughout access points and clients can be difficult and prone to gaps depending on the size of the wireless network. Most importantly, PSK is susceptible to dictionary attacks.</p>	8



<b>Wireless Security Precaution</b>	<b>Related PCI Data Security Standard Requirement</b>
Physically secure wireless APs.	9.1.3
Implement a solution to centrally manage wireless networks, including logging and monitoring. A central management solution provides tighter control, increased automation and greater security.	10
Perform periodic wireless scanning to identify rogue or insecure wireless APs.	11.1

**For more information on Visa's Cardholder Information Security Program, please visit <http://www.visa.com/cisp>. Questions about this bulletin may be directed to [CISP@Visa.com](mailto:CISP@Visa.com).**