

# Visa U.S.A. Cardholder Information Security Program ("CISP") - *Wireless Security Update*

In Brief: With the implementation of new technologies, such as wireless, it is critical to establish proper safeguards to protect cardholder data and maintain compliance with the PCI Data Security Standard. This article is intended to outline the risks associated with wireless technology and offer guidance in mitigating those risks.

---

## Wireless Security

The use of wireless technology is on the rise among participants in the payment industry, particularly retailers, many of whom use wireless for inventory systems or check-out efficiency (e.g., line busting). Since wireless technologies may be susceptible to compromise, merchants are encouraged to carefully evaluate the need for the technology against the risk before deploying wireless systems.

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 should be implemented.

Recent forensic investigations reveal that many entities are not properly securing their wireless networks, which increasingly leads to the compromise of cardholder data, brand damage, and financial and regulatory concerns. Merchants are encouraged to consult with IT staff to ensure proper awareness of the security risks associated with wireless technology and to develop risk mitigation strategies to protect their computing environments.

### Common Wireless Vulnerabilities

- 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.
- Trust problems – 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.
- 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 a business’ operations or to gather additional information for use in initiating another 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.

# Visa U.S.A. Cardholder Information Security Program ("CISP") - Wireless Security Update

## Wireless Security Strategy

Entities that have implemented or are considering implementing wireless technology should develop a comprehensive strategy to secure the environment. The following is a wireless security checklist to consider in conjunction with the PCI Data Security Standard (DSS) and other security strategies.

<b>Wireless Security Checklist</b>	<b>Related PCI DSS Requirement</b>	<input checked="" type="checkbox"/>
Utilize network segmentation to protect assets. The credit card processing environment must be segmented from public networks, including wireless networks, such 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, and</li> <li>• Physical separation of network traffic of different security levels.</li> </ul>	1.3	<input type="checkbox"/>
Implement strong Access Control (ACLs) router rules. ACLs will help to block traffic on known ports, which should not be present on the protected network.	1.3	<input type="checkbox"/>
Always change the vendor-supplied defaults, as follows: <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 SSIDs (Service Set Identifier) 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	<input type="checkbox"/>
Disable all insecure and nonessential management protocols on the wireless AP.	2.2.2	<input type="checkbox"/>
Enable two-factor authentication for the management interfaces of wireless APs and use SSL/TLS for web-based management.	2.3 and 8.3	<input type="checkbox"/>
Implement Wi-Fi Protect Access (WPA) or WPA2 to encrypt transmissions. Never rely on 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). WPA and 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.	4.1.1	<input type="checkbox"/>
Keep security patches on the wireless APs up to date.	6.1	<input type="checkbox"/>
Make sure reset functions on the wireless APs are used only when needed and can only be invoked by authorized individuals.	7.1	<input type="checkbox"/>
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.	8	<input type="checkbox"/>



# Visa U.S.A. Cardholder Information Security Program ("CISP") - *Wireless Security Update*

Physically secure wireless APs.	9.1.3	<input type="checkbox"/>
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	<input type="checkbox"/>
Perform periodic wireless scanning to identify rogue or insecure wireless APs.	11.1	<input type="checkbox"/>

## For More Information

For additional information about CISP or the PCI Data Security Standard, visit the CISP Web site at [www.visa.com/cisp](http://www.visa.com/cisp) or email [AskVisaUSA@visa.com](mailto:AskVisaUSA@visa.com).