# Visa U.S.A. Inc. Data Security Brief

October 5, 2007

To support compliance with the Payment Card Industry Data Security Standard ("PCI DSS"), Visa USA is committed to providing information on how to remedy critical security vulnerabilities. In support of this effort, Visa USA issues Data Security Briefs when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

## Security Vulnerability

### *Improperly Secured Wireless Networks*

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 control systems or checkout efficiency. 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, prior to deploying a wireless system.

Wireless networks should always be considered "untrusted," and Visa highly recommends that security controls be implemented on all such networks, regardless of their purpose. Furthermore, if wireless technology is used to transmit cardholder data, or if a wireless Local Access Network ("LAN") is connected to a part of the cardholder environment, wireless security features must be implemented.

### *Risk Impact*

Payment system participants should be aware of the following methods often used to attack wireless networks. All of these exploits are easily learned by fraudsters as they 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, and the sender, or intended receiver, is unaware 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 control
- Denial of Service — Due to the nature of radio transmission, wireless LANs are vulnerable to denial-of-service ("DOS") 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.

## Recommended Mitigation Strategy

To safeguard wireless networks, payment system participants are encouraged to adopt the following practices:

- Utilize network segmentation to protect assets. The payment-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.
- 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.
- Always change the vendor-supplied defaults as follows:
  - Change default passwords. Default passwords for popular wireless devices are well known to hackers and are often available on the Internet.
  - Change default Service Set Identifier ("SSID") on the wireless Access Point ("AP"). An SSID can be "sniffed" in plain text from a wireless network. SSID character strings should not reflect a name or company identifier.
  - Disable SSID broadcast.
- Encrypt wireless transmissions by using Wireless Fidelity Protected Access ("WiFi WPA" or "WPA2") technology, Internet Protocol Security ("IPSEC") Virtual Private Network ("VPN") or Secure Sockets Layer / Transport Layer Security ("SSL/TLS"). Never rely exclusively on Wired Equivalent Privacy ("WEP") to protect confidentiality and access to a wireless LAN.
- Implement a solution to centrally manage wireless networks, including logging, monitoring and periodic wireless scanning to identify rogue or insecure wireless devices. This solution should ensure that APs are managed within the network, provide strong and secure access controls and automate alerts or reports.

For more information on Visa's Cardholder Information Security Program (CISP), please visit **www.visa.com/cisp**.