

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

May 9, 2007

To support compliance with the Payment Card Industry Data Security Standard (PCI DSS), Visa USA is committed to helping members and payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues security briefs when emerging vulnerabilities are identified in the marketplace, or as a reminder about best practices.

Members may share this brief with their merchants, agents and other parties to help ensure they are aware of emerging vulnerabilities, and take steps, where appropriate, to mitigate risk.

Security Vulnerability

Default Settings/Passwords

As previously reported, merchants using default settings and passwords to access systems components may be susceptible to compromise. New hardware devices and software generally arrive from vendors configured with default settings for ease of installation and management. These default settings must be changed prior to deployment into the production environment as they can be easily guessed and information about these settings is often available on the Internet.

Examples of devices and software that use default settings include the following: routers, switches, servers, wireless access points, shopping carts, point-of-sale (POS) software, Web servers, and database software.

Visa has been made aware of several breaches where the default database password was left blank, thereby providing an easy access point into the database, allowing credit card data stored within the database to be compromised.

Additionally, compromises have occurred when merchants permit vendors to access their POS systems remotely (for maintenance/support), and hackers subsequently access the system because the vendor used a default setting to control entry.

Recommended Mitigation Strategy

To safeguard against the compromise of Visa account information caused by the use of default settings, merchants and agents should take the following actions:

- Check vendor manuals and Internet resources for default settings for all devices and software, and immediately change the default settings upon installation. This includes changing default passwords to a unique, secure password, and changing default account names to custom names as appropriate.
- All unnecessary services should be disabled.
- Merchants should also ensure that all necessary security functions for all devices and software are activated.
- Use the latest version of remote access software and implement the security features according to manual instructions. For example:
 - Ensure that vendors accessing the system remotely change default settings in the remote access software
 - Allow connections only from specific (known) IP/MAC addresses
 - Use strong authentication or complex passwords for logins
 - Enable encrypted data transmission
 - Enable account lockout after a certain amount of failed login attempts
 - Configure the system so a remote user must establish a VPN connection via a firewall before access is allowed
 - Ensure the logging function is enabled
- Use payment applications and versions that have been validated by Visa USA's Payment Application Best Practices (PABP). A list of PABP-compliant applications is available at <http://www.visa.com/cisp>.

**For more information on Visa's Cardholder Information Security Program,
please visit <http://www.visa.com/cisp>**