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

July 31, 2006

To support compliance with the Visa U.S.A. Cardholder Information Security Program, Visa is committed to helping all payment system participants better understand their responsibilities related to securing cardholder data. As part of this commitment, Visa issues security alerts when potential vulnerabilities are detected in the marketplace.

Members may share this alert 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

It has come to the attention of Visa that compromises of card account information have occurred when hackers exploit vulnerabilities created when merchants use vendor default settings / passwords ("default settings") to access hardware devices and software applications.

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 readily guessed and information about these settings is often available on the Internet.

Examples of devices and software that use default settings include: routers, switches, servers, wireless access points, shopping carts, POS software, web server and database software.

Visa has observed compromises where the default database password was left blank, thereby providing an easy access point into the database and credit card data stored within. Additionally, compromises have occurred when merchants permitted vendors to remotely access their POS systems (for maintenance / support) and hackers subsequently accessed the system because a default setting was used by the vendor 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 turned on.
- Use the latest version of remote access software, and implement the security features per the manual. 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 number of failed login attempts.
  - Configure the system so a remote user must establish a Virtual Private Network ("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.

Alert 073106