



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

May 22, 2006

To support compliance with the Cardholder Information Security Program, Visa U.S.A. is committed to helping members and payment system participants better understand their responsibility to secure cardholder data. As part of this commitment, Visa will be issuing security alerts when significant vulnerabilities are detected in the marketplace.

Members may share this alert with their merchants and agents as a confidential communication to help ensure they learn about emerging vulnerabilities and take steps where appropriate to mitigate risk.

Security Vulnerability

SQL Injection Attacks

SQL injection is a technique used to exploit web-based applications that use client-supplied data in SQL queries. SQL injection attacks may be the by-product of un-patched web servers, an improperly designed application, or poorly configured web servers and database servers.

A review of recent data security breaches suggests SQL injection attacks on e-commerce merchants have become more prevalent. The attack method most recently detected targets shopping carts that are not properly patched and are therefore susceptible to attack.

Recommended Mitigation Strategy

Members are encouraged to share the information below with their merchants and agents. To minimize the possibility of an SQL attack, merchants should take the following actions:

- Use only a secure shopping cart, preferably validated against Visa's Payment Application Best Practices ("PABP"). A list of PABP compliant shopping carts is available on <http://www.visa.com/cisp>.
- Test susceptibility to SQL injection utilizing automated tools or manual techniques.
- Merchants that utilize proprietary or custom applications should adopt secure coding practices that include independent code reviews.
- Use only secure web servers. Merchants can refer to their vendor's website for instructions on hardening web servers (See Microsoft's website on hardening IIS servers using IIS lockdown tools <http://www.microsoft.com/technet/security/tools/locktool.mspx>).
- Ensure web servers are routinely updated with the current security patches from their vendors.
- Purge cardholder data when no longer needed and take steps to ensure CVV2 data is not stored subsequent to authorization of a transaction.

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

Alert 052206