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

June 6, 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 Data 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

### *SQL Injection Attacks*

A review of recent data security breaches suggests Sequel (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.

Visa first published a Data Security Brief on this issue in May 2006. However, since SQL injection continues to be a prominent attack method, this brief is being re-published to remind payment system participants of this vulnerability.

SQL injection is a technique used to exploit Web-based applications that use client-supplied data in SQL queries. SQL injection attacks can occur as a result of un-patched Web servers, improperly designed applications (incorrectly filtered escape characters or error-type handling), or poorly configured Web and database servers.

### *Recommended Mitigation Strategy*

To minimize the possibility of a SQL attack and mitigate the risk of a data compromise, merchants should take the following actions:

- Use only a secure shopping cart validated by Visa's Payment Application Best Practices (PABP). A list of PABP-compliant shopping carts is available on *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 Web site for instructions on hardening Web servers. (For an example, visit *www.microsoft.com* for instructions on hardening IIS servers using IIS lockdown tools.)
- 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 following authorization of a transaction.

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