



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

April 5, 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 responsibility to secure 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 payment participants to help ensure they learn about emerging vulnerabilities and take steps where appropriate to mitigate risk.

Security Vulnerability

Enabling Audit Logging

An important requirement of PCI DSS compliance is the tracking and monitoring of all access to network resources and cardholder data. In the case of a system intrusion, the ability to track user activities is crucial. The presence of system activity logs allows forensic investigators to thoroughly track and analyze suspicious activity or confirmed intrusions. Determining the cause and time span of a compromise is more difficult, or in some cases impossible, without these audit logs.

Recommended Mitigation Strategy

Complete log files are critical to the successful investigation and prosecution of security incidents, therefore best practices recommend enabling logging for all events. The audit trail entries for all system components should include user ID, type of event, date and time, success or failure indication, origination of event and identity of the system component.

Retention of the audit logs is a vital aspect of PCI DSS compliance, which requires companies to retain audit trail history for at least one year, with a minimum of three months available online.

In addition to retention requirements, log files must be secured and access restricted and monitored. In an attempt to conceal unauthorized access or attempted access, intruders will try to edit or delete log files. Efforts to secure log files should include:

- Limit viewing of audit trails to those with a job-related need.
- Protect audit trail files from unauthorized modifications.
- Segregate logged data to an independent server.
- Use file integrity monitoring/change detection software to ensure existing log data cannot be changed without generating alerts.

Log harvesting, parsing and alerting tools may be used to meet PCI DSS compliance. A good log management solution should provide a scalable and centralized process that can collect, normalize, aggregate, compress and encrypt log data from disparate sources such as routers, switches, firewalls, IDS/IPS, AV, SPAM/spyware, Windows, UNIX and Linux systems. This helps to identify security breaches, hacker intrusion and/or any other activity that could potentially be crippling to valuable corporate assets.

A good log management solution should also automate the process of producing reports, with relevant information that will identify an anomaly or glitch. Staff should review logs for all system components at least daily.

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