

# Visa Inc. Data Security Brief

## Enabling Audit Logging

August 29, 2008



In accordance with the Payment Card Industry Data Security Standard (PCI DSS) and to promote the security and integrity of the payment system, Visa Inc. is committed to helping clients and payment system stakeholders better understand their obligation to protect cardholder information. 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.

Visa clients are strongly encouraged to share this updated brief with their merchants, agents and other payment system stakeholders to promote awareness of these threats and ensure that appropriate steps are taken to mitigate risk.

### Security Vulnerability

#### **Enabling Audit Logging**

Requirement 10, an important requirement of PCI DSS compliance, calls for the tracking and monitoring of all access to network resources and cardholder data. The ability to track user activities is crucial in the event of a system intrusion. The presence of system activity logs allows security personnel and forensic investigators to thoroughly track and analyze suspicious activity or confirm intrusions. Determining the cause and timeline of a data compromise is more difficult, or in some cases impossible, without the use of audit logs.

#### **Recommended Mitigation Strategy**

Complete log files are critical to the successful investigation and prosecution of security incidents. Security 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.

The retention of audit logs is a key requirement of PCI DSS compliance. PCI DSS requirement 10.7 requires companies to retain audit trail history for at least one year, with a minimum of three months available online. In addition, PCI DSS requirements 10.5.1-10.5.5 specify that log files must be secured with access restricted and monitored.

In an attempt to conceal unauthorized access or attempted access, intruders will try to edit or delete log files. To secure log files:

- 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. Sources may include (but should not be limited to) the following system components: routers, switches, firewalls, intrusion detection and prevention systems, antivirus, spam, spyware / malware, Windows, UNIX and Linux systems. These sources will help identify security breaches, hacker intrusion and/or any other activity that could cripple valuable corporate assets.

A good log management solution should also automate the ability to produce reports containing relevant information that will indicate an anomaly or glitch. Lastly, logs for all system components should be reviewed at least daily.

**For more information or for answers to questions regarding the information in this brief, please visit [www.visa.com/cisp](http://www.visa.com/cisp) or e-mail [cisp@visa.com](mailto:cisp@visa.com).**