



Visa Inc. Data Security Alert for Hospitality Merchants

January 9, 2009

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 in accordance with the Payment Card Industry Data Security Standard (PCI DSS). As part of this commitment, Visa issues Data Security Alerts when emerging vulnerabilities are detected in the marketplace.

Visa clients are strongly urged to share this alert with their merchants, particularly with hospitality merchants and other payment system stakeholders, to promote awareness of these threats and ensure that immediate steps are taken to mitigate risk.

Cardholder Data in Transit

Recent data security breaches reported to Visa indicate that criminals continue to target merchants in the hospitality industry, specifically hotels and restaurants. With the secure implementation and use of Payment Application Data Security Standard (PA-DSS) compliant applications, attacks upon data at rest have become more difficult. Criminals have shifted their attacks to intercept cardholder data in transit during transaction authorization through the use of packet sniffers, memory parsers and other malware. Further information on these attack methods, specific variants identified in data security breaches, and mitigation strategies can be found on Visa's website at www.visa.com/cisp under *Alerts, Bulletins and Webinars*.

Packet sniffers, memory parsers and other malware pose serious risks when installed on critical systems because they can allow criminals to penetrate the cardholder data network and gain entry into merchants' systems. Once network intruders gain entry, they can steal cardholder data and identification of the incident is difficult to detect. These threats underscore the urgency of maintaining compliance with all PCI DSS requirements.

Signs of a Suspected Breach

Although detection can be difficult to identify, any sign of a suspected security incident requires that Visa clients and their merchants take immediate action to investigate the incident, limit the exposure of cardholder data, notify Visa and report investigation findings. Instructions for these procedures can be found in Visa's [What to Do If Compromised](#) document. Signs of an incident include the following, but are not limited to:

- Failed log-in attempts in system authentication and event logs
- Unexplained modification or deletion of data, including changes in file lengths and dates
- Presence of unexpected IP addresses on merchant networks, including wireless
- Unknown or unexpected user accounts, services or applications
- Presence of compressed or uncompressed files (e.g., .zip, .rar, .tar, .log) containing cardholder data

Recommended Mitigation Strategy

To minimize the possibility of a data security breach and mitigate the risk of a data compromise, merchants should maintain PCI DSS compliance and, at a minimum, take the following actions:

- Implement a firewall to permit network traffic only where there is a defined business need and deny all other network traffic
- Use and securely implement PA-DSS compliant applications and update all systems routinely with current security patches
- If use of remote access products is necessary, implement the latest security patches and configurations, and ensure strong authentication is required for log in
- Ensure antivirus, anti-spyware and anti-malware software are up-to-date
- Contact product vendors for more information on how to secure their products

For more information on securing cardholder data, please visit <http://www.visa.com/cisp>.