PCI Security Standards Council

Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI Security Standards Council Statement on Recent Data Breaches
July 27 2009

Until a forensics investigation is completed, an organization can not comment accurately on its compliance status.

Friday's announcement of a data breach at Network Solutions underscores the necessity for ongoing vigilance of an organization's security measures. Security doesn't stop with PCI compliance validation. As the Council has said many times, it is not enough to validate compliance annually and not adopt security into an organization's ongoing business practices. A card data environment is under constant threat, so businesses must ensure their safeguards are also under constant vigilance, monitoring and where necessary, ongoing improvement. A layered approach to security is absolutely necessary to protect sensitive payment card data – without ongoing vigilance or a comprehensive security strategy, organizations may be just a change control away from noncompliance.

Validation to the principles and practices mandated in the PCI DSS plays an integral part in an organization's security posture, but basic monitoring and logging cannot be set aside after a security assessment is complete. Reports by forensics companies suggest that this is an area of weakness among organizations. An intrusion need not result in card data compromise if an organization is following the 12 guiding requirements of the PCI Data Security Standard.