PCI: 5 New Security Requirements

Original email dated 6.3.15

The five best practices noted in **version 3.0** of *the PCI Data Security Standard* will become requirements after June 30, 2015. Most likely to be affected will be smaller merchants. New requirements relate to point-of-sale vulnerabilities that have been linked to activities at small and mid-sized businesses.

The best practices, which were included when PCI-DSS version 3.0 was released in November 2013, are as follows:

1. Merchants should secure authentication and online session management to help prevent the theft of online credentials;
2. Third-party service providers with remote access to POS systems should use a unique passcode credential for each merchant customer;
3. Service providers should confirm in writing that they are responsible for the security of cardholder data they store, process or transmit on behalf of the merchant;
4. Merchants should regularly inspect POS devices to ensure that they have not been "swapped" or tampered with to skim or collect card details;
5. Merchants should conduct regular penetration testing through simulated device attack scenarios to exploit known and possible vulnerabilities.

The PCI Security Standards Council says merchants of all sizes are increasingly at risk and that these requirements reflect areas all businesses should address.

Attack trends suggest that smaller merchants will continue to face more breaches than larger organizations.

Please keep this information in mind as it relates to the PCI requirements at your site.