



Read This If You Accept Payment Cards

PCI Updates Payment Card Data Security Standard

By: Patrick J. Hatfield, Louis Dienes, and Vita E. Zeltser

The PCI Security Standards Council (PCI SSC), an organization that develops standard for payment card security, recently published an updated version of the Payment Card Industry Data Security Standards (PCI DSS), applicable to all entities involved in the payment card process, including merchants that accept payment cards. The new version, Version 3.0, which can be accessed by [clicking here](#), becomes effective on January 1, 2014, and companies will have one year to become compliant. An updated version of the Payment Application Data Security Standards, applicable to certain software vendors and others who develop card payment applications, was also issued by the PCI SSC.

PCI DSS compliance is required by all merchant agreements, and constitutes a critical step in mitigating the risks for data security breaches.

According to the PCI SSC, the goal of Version 3.0 of the Data Security Standards is to “help organizations make payment security part of their business-as-usual activities by introducing more flexibility, and an increased focus on education, awareness and security as a shared responsibility.”

Importantly, the updated PCI DSS clarifies that liability for PCI compliance cannot be outsourced. Companies that accept payment cards but that outsource all card processing functions still have important compliance obligations. Thus, all companies that accept or process payment cards should review the new standard to ensure that they and their vendors are compliant.

For more information on the matters discussed in this *Locke Lord QuickStudy*, please contact the authors:

Patrick J. Hatfield | 512-305-4787 | phatfield@lockelord.com

Louis Dienes | 213-687-6737 | ldienes@lockelord.com

Vita E. Zeltser | 404-870-4666 | vzeltser@lockelord.com