MorrisonCohen LLP

Law Firm to the Middle Market®

Credit Card Council Raises Cybersecurity Standards

May 3, 2016 – Responding to increased concern over the security of personal financial data, the Payment Card Industry Security Standards Council last week released a set of heightened access standards for all payment card processors.

Under the new standards, called PCI DSS v. 3.2, anyone handling credit card data must require at least two of three different types of authentication before granting anyone administrator access to the cardholder data environment, and to anyone seeking to access data remotely (including logins by third parties, as well as logins from other networks within the same facility). The PCI DSS considers the three authentication factors to be: (i) something you know, such as a password; (ii) something you are, such as biometrics; and (iii) something you have, such as a token.

This new requirement will be considered best practices until January 31, 2018, after which it will become mandatory.

The Council has made some additional clarification changes in the PCI DSS in this new version 3.2 as well, all effective immediately, including clarifying that: (i) backup sites must be taken into consideration when confirming the scope of a PCI compliance review; (ii) payment application vendor-supplied passwords must be modified prior to use; (iii) only parties with a legitimate business need may see a display of more than the first six digits or the last four digits of the primary account number; (iv) all security patches to payment application software must be made in a timely manner, as well as other software in the cardholder data environment; (v) training for software developers in up-to-date secure coding techniques must occur at least annually; and (vi) the security of backup media storage facilities must be evaluated at least annually.

Companies handling credit card data, including service providers and retailers, have seen a surge in consumer-initiated litigation resulting from security breaches and resulting threats to personal, financial and data integrity. Compliance with PCI DSS is not only required by all financial institutions clearing credit card transactions for businesses, but also by those who process, transmit, store or otherwise collect credit card data. It is also important for investment funds and other investors evaluating a transaction with enterprises that handle PCI data, to take steps to ensure that the target is complying with the new standard.

For further discussions regarding new PCI DSS v. 3.2, or any other privacy or data security issue, please contact your personal Morrison Cohen attorney, or:

David Lerner
(212) 735-8609
DLerner@morrisoncohen.com

Jessica L. Lipson
(212) 735-8683
Jlipson@morrisoncohen.com