Kelley Drye

FTC Requests Auditors’ Data on PCI Data Security Assessments

Alysa Z. Hutnik

March 9, 2016

Earlier this week, the FTC issued orders to nine credit card and payment security auditors in an effort to gain insight into data security compliance auditing and its role in protecting consumers’ information and privacy.

The orders contain detailed questions concerning the assessment process for Payment Card Industry Data Security Standard (“PCI DSS”) compliance, including the policies and procedures in place to govern the assessment, and the percentage of clients that have been found to be non-compliant. In addition, the orders request information on whether the auditors provide any data security forensic audit services, and the processes and procedures in place for doing so. The Commission is also requesting information on whether the auditors have been the subject of any government or regulatory inquiry, private action, arbitration, or mediation related to any of its PCI DSS services.

So What Does This Mean? The Commission has not specified exactly what it plans to do with the data collected, other than to say that it “will be used to study the state of PCI DSS assessments.” As a general matter, all merchants are bound to comply with PCI DSS through a merchant agreement executed between the merchant and its merchant bank. Some states have also codified portions of the PCI DSS to require certain protections for PCI. Nonetheless, a significant amount of data breaches still involve the compromise of payment card information, and some of these breaches have occurred by merchants that are certified as PCI-compliant at the time of the attack.

The auditors have been ordered to respond by mid-April, so be sure to stay tuned for next steps from the FTC.