

Revised Data Security Standards for Payment Cards

May 25, 2016

The Payment Card Industry Security Standards Council recently released revised data security standards for payment cards, which include debit cards issued by vendors in conjunction with flexible spending accounts, health reimbursement arrangements, and health savings accounts. These revised standards update the Payment Card Industry Data Security Standard (PCI DSS) to version 3.2 and contain a variety of enhancements to protect against security threats, including revised system penetration testing requirements, enhanced policies and procedures for detecting failures, and stricter authentication protocols. The PCI DSS responsibilities fall on the card issuers, vendor service providers, merchants, etc., not on an employer which merely sponsors or facilitates a spending account benefit that utilizes debit cards. PCI DSS version 3.2 will be viewed as a "best practice" until January 31, 2018. Beginning February 1, 2018, version 3.2's standards become mandatory for the industry. Employers sponsoring or facilitating spending account benefits utilizing debit cards should update their requests for proposals from spending account service providers by inquiring when the service provider will become PCI DSS version 3.2 compliant. Employers may also receive periodic updates from their existing service providers about system enhancements toward compliance. The revised standards and a summary of changes are available [here](#).