Published on *The National Law Review* https://natlawreview.com

Just Released: New Version of Global Standard for Payment Card Data Security

Article By:

Edward J. Hansen

Christopher C Archer

On April 28, the ***Payment Card Industry (PCI)*** Security Standards Council (Council) announced the release of PCI Data Security Standard (PCI DSS) version 3.2 to replace version 3.1, which expires on October 31, 2016. The announcement states that "[c]ompanies that accept, process or receive payments should adopt [version 3.2] as soon as possible to prevent, detect and respond to cyberattacks that can lead to breaches."

The Council pointed out that because PCI DSS is recognized as a "mature standard" by the payment industry, "the primary changes in version 3.2 are clarifications on requirements that help organizations confirm that critical data security controls remain in place throughout the year, and that they are effectively tested as part of the ongoing security monitoring process."

One such change is to expand the use of multi-factor authentication to include all administrators who access cardholder data. This builds on the existing requirement of multi-factor authentication for all personnel with remote access to cardholder data.

Version 3.2 also includes a number of new requirements for organizations to follow, most of which apply only to service providers. To allow companies time to implement the new requirements, they will serve as best practices until January 31, 2018, after which they will become requirements.

Highlights of the new requirements include the following:

- New requirement 3.5.1 — Service providers must maintain a documented description of cryptographic architecture (e.g., algorithms, protocols, and keys).
- New requirement 6.4.6 — Organizations must ensure that security controls are implemented and documentation updated for all new or changed systems and networks. In other words, validation of security controls must be incorporated into change management processes.
- New requirements 10.8 and 10.8.1 — Service providers must establish processes to timely detect, report, and respond to failures of critical security control systems (e.g., firewalls, anti-

virus, and physical/logical access controls).

- New requirement 11.3.4.1 — Service providers must perform penetration testing on segmentation controls (if used) every six months (formerly an annual requirement) and after any change to segmentation controls.

- New requirement 12.4.1 — Executive management must establish responsibilities for the protection of cardholder data and implement a PCI DSS compliance program.

- New requirements 12.11 and 12.11.1 — Service providers must perform reviews on at least a quarterly basis to confirm that personnel are following security policies and procedures, and maintain documentation of such quarterly review process.

The Council published a summary of changes in its document library that provides more detail on version 3.2, and the Council's Chief Technology Officer, Troy Leach, discussed the key changes in an interview last week.

Going Forward

The Council expects to continue to release incremental revisions to the PCI DSS standard (like version 3.2) "to address evolving threats to the payment landscape, with a focus on helping companies use this standard as a good framework for everyday security and business best practice."

With more incremental revisions to PCI DSS on the horizon and a constantly evolving threat landscape, companies that accept, process, or receive payments should ensure that security practices and controls remain current and adaptable to changing standards, whether such practices and controls are managed in-house or by a third party. For contracting purposes, strong PCI DSS compliance provisions are critical when a service provider accepts, processes, or receives payments on behalf of a customer. In addition, prior to engaging any such service provider, customers should validate that the solution includes robust PCI DSS practices.

National Law Review, Volume VI, Number 130