Decoding the new payment card security standard

James J. Giszczak, Dominic A. Paluzzi | Tuesday, March 3, 2015

It's been a little over a year since the latest version of the Payment Card Industry Data Security Standard (PCI DSS) was released. Given the proliferation and severity of data breaches in the last year, the newly released standards will hopefully help mitigate risk of financial fraud when using credit cards. January 1, 2015, was the mandatory deadline for compliance with PCI DSS Version 3.0. This alert summarizes what businesses, including merchants, subject to PCI DSS Version 3.0 need to know.

What is PCI DSS and what businesses must comply?

The PCI DSS is a proprietary information security standard for organizations that handle branded credit cards from the major card brands including Visa, MasterCard, American Express, Discover, and JCB. Private label cards, *i.e.,* those without a logo from a major card brand, are not included in the scope of the PCI DSS. The PCI Standard is mandated by the card brands and run by the Payment Card Industry Security Standards Council, which was created to increase controls around cardholder data to reduce credit card fraud via its exposure.

Each of the five major credit card companies had their own programs, but after the Payment Card Industry Security Standards Council was formed in 2004, each company unified their individual policies and released version 1.0 of the PCI DSS. Since then, PCI DSS has been amended five times (version 1.1, 1.2, 1.2, 1.2.1, 2.0 and 3.0). The most recent version is 3.0, and it was released in November 2013. This version is active from January 1, 2014 to December 31, 2017.

Why is PCI DSS important?

PCI DSS includes a prioritized approach with six milestones to help organizations incrementally protect against the highest risk factors while they still obtain PCI DSS compliance. The milestones are aimed to help entities take a risk-based approach to PCI compliance, and are as follows:

Milestone	Goals
1	**Remove sensitive authentication data and limit data retention.** If sensitive authentication data and other cardholder data are not stored, the effects of a compromise are significantly reduced.
2	**Protect systems and networks, and be prepared to respond to a system breach.** Targets controls for points of access to most compromises, and the processes for responding.
3	**Secure payment card applications.** Targets controls for applications, application processes, and application servers.
4	**Monitor and control access to your systems.** Allows for the detection of what, when, how, and who accessed a network and cardholder data.
5	**Protect stored cardholder data.** For organizations that have analyzed their business processes and determined they must store Primary Account Numbers, this focuses key protection mechanisms for that stored data.
6	**Finalize remaining compliance efforts, and ensure all controls are in place.** The purpose is to complete PCI DSS requirements, and finalize all remaining related policies, procedures, and processes needed to protect the cardholder data environment.

What are PCI DSS's objectives and requirements?

PCI DSS outlines 12 requirements for compliance that are organized into six groups of control objectives.

Control Objectives	PCI DSS Requirements
Building and Maintaining a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data.
	2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data.
	4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability	5. Use and regularly update anti-virus software on all systems commonly affected by malware.
	6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know.
	8. Assign a unique ID to each person with computer access.
	9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data.
	11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security.

When the most recent version, PCI DSS **3.0** was rolled out, it contained 98 total changes from version 2.0. A 12-page summary outlining the differences between PCI DSS version **2.0** to **3.0** can be found **here**. A concise highlight document summarizing version 3.0 is available **here**.

While "98 total changes" sounds a tad daunting, most are just clarification-related and supplemental, not new requirements. Of the 19 new requirements, which amount to about 20% of version 3.0, most are borne out of the new technology merchants and attackers are using.

One large change for service providers is that they must explicitly attest to their compliance and provide a copy of their attestation to their customers. While nothing in it indicates they assume liability, it is assumed since they will now have to attest to their PCI compliance.

Below are the 19 *new* requirements:

New Requirement
Req. 1.1.2 and 1.1.3 – Clarified what the network diagram must include and added a new requirement at **1.1.3** for a current diagram that shows cardholder data flows.
Req. 2.4 – Maintain an inventory of system components in scope for PCI DSS to support development of configuration standards.
Req. 5.1.2 – Evaluate evolving malware threats for any systems not considered to be commonly affected.
Req. 5.3 – Ensure that anti-virus solutions are actively running (formerly in **5.2**), and cannot be disabled or altered by users unless specifically authorized by management on a per-case basis.
Req. 6.5.10 – Coding practices must protect against broken authentication and session management. *Effective July 1, 2015.*
Req. 8.2.3 – Combined minimum password complexity and strength requirements into a single requirement, and increased flexibility for alternatives that meet the equivalent complexity and strength.
Req. 8.5.1 – New requirement for service providers with remote access to customer premises to use unique authentication credentials for each customer. *Effective July 1, 2015.*
Req. 8.6 – Where other authentication mechanisms are used, e.g., physical or logical security tokens, smart cards, certificates, etc., the mechanisms must be linked to an individual account and ensure only the intended user can gain access with that mechanism.
Req. 9.3 – Control physical access to sensitive areas for onsite personnel, including a process to authorize access, and revoke access immediately upon termination.
Req. 9.9.x – Protect devices that capture payment card data via direct physical interaction with card from tampering and substitution. *Effective July 1, 2015.*
Req. 10.2.5 – Implement automated audit trails for all system components to reconstruct the following events; Changes to identification and authentication mechanisms (including creation of new accounts, elevation of privileges), and all changes additions and deletions to accounts with root or administrative access.
Req. 10.2.6 – Implement automated audit trails for all system components to reconstruct the following events: initiating, stopping or pausing of the audit logs.
Req. 11.1.x – Enhanced requirements to include an inventory of authorized wireless access points and a business justification (**11.1.1**) to support scanning for unauthorized wireless devices, and added new requirements **11.1.2** to align with an already-existing testing procedures, for incident response procedures if unauthorized wireless access points are detected.
Req. 11.3 – Implement a methodology for penetration testing. *Effective July 1, 2015. PCI DSS v. 2.0 requirements for penetration testing must be followed until v. 3.0 is in place.*
Req. 11.3.4 – If segmentation is used to isolate the CDE from other networks, perform penetration tests to verify that the segmentation methods are operational and effective.
Req. 11.5.1 – Implement a process to respond to any alerts generated by the change-detection mechanism (supports **11.5**).
Req. 12.2 – Moved former requirements **12.1.2** for an annual risk assessment process to **12.2**, and clarified that the risk assessment should be performed at least annually and after significant changes to the environment.
Req. 12.8.5 – Maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.
Req. 12.9 – For service providers to provide the written agreement/acknowledgment to their customers as specified at requirement **12.8**.

Takeaways

Five key areas will likely be the most dramatic for merchants:

1. Penetration testing, which is the visible change to the existing requirements
2. Inventorying system components
3. Vendor relationships
4. Anti-malware
5. Physical access and point of sale

Keep in mind that Target and The Home Depot were deemed to be “PCI” compliant at the time of their respective massive data breaches. It’s important to remember that even compliance with the new PCI DSS 3.0 does not shield an organization from a data breach. Although PCI compliance is important (and required for many organizations), conducting a broader risk assessment and implementing privacy safeguards across the organization will be even more effective.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Dominic A. Paluzzi