BNA

Privacy & Security Law Report®

Contracting for PCI DSS Compliance in the Cloud



BY RANDALL S. PARKS, ANDREW G. GEYER, MELINDA L. MCLELLAN AND EFE STELLA EDOSOMWAN

Introduction

As merchants move to reap the functional and operational benefits of virtualized environments, compliance with the Payment Card Industry Data Security Standard (PCI DSS) is becoming increasingly complicated, yet all the more essential to the protection of cardholder data. In addition to the formidable threats posed by the physical infrastructure of client-server computing, the complexity of virtual environments creates unique security challenges for merchants processing sensitive information on virtual machines over which they have only limited control. Although many merchants have outsourced data storage and processing to third parties, ultimate responsibility for securing customer data remains with the merchant. This article discusses the PCI DSS compliance requirements of merchants and cloud providers, and suggests a framework for contracting for that compliance.

Randall S. Parks is the Co-Chair of the Global Technology, Outsourcing and Privacy practice group at the Richmond, Va. law office of Hunton & Williams LLP. Andrew G. Geyer is an associate with the group in Richmond, Va. and Melinda L. McLellan is an associate with the group in New York. Efe Stella Edosomwan is a student at the Washington University in St. Louis School of Law.

New Guidance for Complying with PCI Data Security Standard Has Significant Implications for Merchants and Cloud Providers

On June 14, the Virtualization Special Interest Group of the PCI Security Standards Council published its *PCI DSS Virtualization Guidelines Information Supple-*

 ISSN 1538-3423

ment[1] to Version 2.0 of the PCI DSS. For merchants (defined broadly as any entity that accepts payment cards bearing the logos of PCI Security Standards Council members American Express, Discover, JCB, MasterCard or Visa), the Guidelines make clear that unquestioning reliance on a service provider's assertion of PCI compliance is inadequate and risky. For cloud providers, the increased focus on applying the PCI DSS in virtual environments means they must prepare to respond to customer questions and convincingly demonstrate their ability to comply.

As the Guidelines point out, new vulnerabilities in virtualized environments can threaten an individual virtual machine that may itself be secure. The consolidation of resources inherent in virtual environments increases the risk that a single point of failure will expose multiple customers. On a more basic level, failure to comply with the PCI DSS also may jeopardize a merchant's ability to process credit card transactions. The stakes are further increased by the emergence of state data security laws that incorporate the PCI DSS in its entirety. Nevada's law on the Security of Personal Information, for example, requires that merchants doing business in Nevada and accepting payment cards must comply ''with the current version of the Payment Card Industry (PCI) Data Security Standard, as adopted by the PCI Security Standards Council'' (NRS Chapter 603A) (8 PVLR 821, 6/8/09). See our Client Alert[2] on this topic.

The Guidelines not only provide context for the application of the PCI DSS to cloud and other virtual environments, they also include at least three critical reminders: *first,* the PCI DSS applies to those environments without exception; *second,* critical analysis of the application of the PCI DSS to rapidly evolving cloud offerings is essential to compliance; and *third,* cloud providers must be prepared to include necessary controls in their contracts. The Guidelines offer high-level vocabulary and technical advice, cataloging common components of virtualized environments and identifying those that are likely to be ''in scope'' for PCI DSS purposes. A number of recommendations and suggested best practices are included in the Guidelines, most of which focus on the critical need for precise technical understanding of how each virtual environment operates with respect to cardholder data as an essential first step in assessing PCI DSS compliance. To facilitate compliance, the Guidelines also include an appendix that provides a detailed list of virtualization considerations relevant to each of the 12 requirements of the DSS. Of particular relevance to cloud offerings, the Guidelines emphasize the importance of ensuring that the service offering is able to isolate each customer's environment using controls such as segmented authentication, network access controls, encryption and logging.

The Guidelines hold cloud providers to a high standard, indicating that customer access to the shared cloud infrastructure is risky, and limiting that sharing requires implementation of ''[m]ore stringent preventive, detective, and corrective controls . . . to offset the additional risk that a public cloud, or similar environment, could introduce.'' Perhaps ominously for some, the Guidelines conclude that ''these challenges may make it impossible for some cloud-based services to operate in a PCI DSS compliant manner.'' Accordingly, the Guidelines state that cloud providers must bear the burden of demonstrating compliance and should be required to provide ''rigorous evidence of adequate controls.'' In particular, the Guidelines state that ''[t]he cloud provider should be prepared to provide their hosted customers with evidence that clearly indicates what was included in the scope of their PCI DSS assessment as well as what was not in scope; details of controls that were not covered and are therefore the customer's responsibility to cover in their own PCI DSS assessment; details of which PCI DSS requirements were reviewed and considered to be in place and not in place; and confirmation of when the assessment was conducted.''

Strategies for Contracting in the Cloud

Outsourcing security and processing functions to a third-party service provider does not relieve a merchant of its responsibility to ensure that cardholder data is protected, regardless of where the data is hosted. Requirement 12.8 of the PCI DSS states that merchants that share cardholder data with service providers must maintain (1) a list of such service providers; (2) written agreements that include an acknowledgement that the service providers are responsible for the security of cardholder data; (3) a process for engaging service providers, including proper due diligence prior to engagement; and (4) a program for monitoring service providers' PCI DSS compliance.

Items (2) and (4) can be addressed contractually. While the specific contractual language may vary depending on commercial elements, at a minimum it should address the following: (1) compliance with the basic tenets of Requirement 12.8; (2) allocation of the responsibility for compliance with the detailed controls mandated by the other PCI DSS requirements; and (3) allocation of responsibility for maintaining compliance throughout the life of the relationship, including how the parties will address changes in technology and in the PCI DSS itself. The model contractual provisions below assume that the provider will accept certain compliance risk (and related costs and duties) for competitive reasons, a stance that is becoming increasingly common, especially among larger providers and those offering high-volume, standardized solutions. More customized solutions may require a more tailored approach. The provisions incorporate PCI DSS requirements indirectly, but some customers may prefer to be more prescriptive. References in the provisions to ''Schedule X'' refer to a separate, more detailed allocation of PCI DSS obligations, which may be useful in some transactions.

Model Contractual Provisions:

(a) Service Provider shall perform the services in compliance with the PCI DSS requirements set forth on Schedule X and elsewhere in the Agreement and acknowledges its responsibility for the security of

[1] The *PCI DSS Virtualization Guidelines Information Supplement* is available at https://www.pcisecuritystandards.org/documents/Rth87Wp/Virtualization_InfoSupp_v2.pdf (10 PVLR 940, 6/27/11).

[2] The Client Alert is available at http://www.hunton.com/files/tbl_s10News/FileUpload44/16384/nevada_updates_encryption_law.pdf

  PVLR ISSN 1538-3423

cardholder data which it stores, transmits or processes.

(b) Service Provider shall perform all tasks, assessments, reviews, penetration tests, scans and other activities required under the PCI DSS (including any compliance guidance issued by the PCI Data Security Council or its subordinate bodies) or otherwise to validate its compliance during the Term with the PCI DSS as it relates to the system elements and portions of cardholder data environment (each as defined by the PCI DSS) for which Service Provider is responsible as set forth in Schedule X (the ''PCI Environment''). Service Provider shall deliver to Customer copies of all documentation necessary to verify such compliance (''Verification Documentation''). In the event Customer reasonably determines that additional Verification Documentation is required under the PCI DSS or likely to be so required to verify such compliance, including a ''Report on Compliance,'' and an associated unqualified ''Attestation of Compliance,'' then, upon Customer's request and at no additional charge to Customer, Service Provider shall provide such additional Verification Documentation to Customer within six (6) months from Customer's request, or the timeframe required for Customer to remain compliant, whichever is less. Notwithstanding the foregoing, should Customer's request for additional Verification Documentation ultimately not be required in order for Customer to demonstrate compliance with the PCI DSS in a manner permitted under the PCI DSS, Customer shall reimburse Service Provider the actual, reasonable costs incurred by Service Provider in connection with such additional Verification Documentation for the relevant time period. At least annually thereafter for so long as Customer reasonably determines that such documentation is required under the PCI DSS, Service Provider shall deliver to Customer a copy of the Verification Documentation, applicable to the PCI Environment at no additional charge to Customer. Within ten (10) Business Days of Customer's request, Service Provider shall deliver to Customer at no additional charge evidence of a passing vulnerability scan applicable to the PCI Environment conducted within the preceding three (3) months. Service Provider will immediately notify Customer of any exception in a Report on Compliance, Attestation of Compliance or quarterly vulnerability scan or if it learns that it is no longer PCI DSS compliant, or reasonably anticipates that it is or will be noncompliant, and will promptly notify Customer of the steps being taken to remediate such exception or non-compliance.

Addressing Changes in Technology and Regulation

Cloud services are evolving rapidly, inspiring equally rapid changes in applicable law and industry standards, such as the PCI DSS. Although regulatory change could be viewed as a sort of *force majeure* that relieves both parties of their obligations and triggers termination or renegotiation, embracing that approach in a dynamic environment leads to unstable relationships and inefficient protective behaviors. A common variation on that theme is limiting the term of the agreement to reduce the likelihood of noncompliance and allow for more frequent renegotiation of compliance duties and pricing. However, many larger providers of standardized offerings are now willing to commit to maintaining long-term compliance with the PCI DSS pursuant to provisions similar to the example below. In more customized relationships, negotiations typically revolve less around the risk of noncompliance and more around allocating the cost of compliance. Contractual language for the standardized approach (with an option to accommodate customization) follows:

''Service Provider shall conform the services in a timely manner to comply with any change in the PCI DSS (including any compliance guidance issued by the PCI Data Security Council or its subordinate bodies), provided that Service Provider shall provide Customer with at least [90] days advance written notice of any such changes, or, if [90] days notice is not possible, then as promptly as practicable following any such change. Such conformance of the services shall be at Service Provider's expense with respect to changes that are applicable generally to Service Provider's other customers for services which are the same as or similar to the services or relevant components of the services. With respect to new or revised Customer compliance requirements that are unique to Customer, Service Provider may propose for Customer's acceptance commercially reasonable changes to the charges which equitably account for any efficiencies, economies or reduced or increased resource requirements resulting from any changes in the services. If Customer accepts such changes, then Service Provider will implement Customer's compliance requirements on a timeline which will enable Customer to comply and, following such implementation, Customer shall pay Service Provider revised charges.''

Conclusion

Merchants who engage third-party cloud providers should consider whether their provider's services are subject to the PCI DSS, and review the assignment of data security responsibilities in their contracts in light of the PCI Security Standards Council's new Guidelines. For their part, service providers should prepare to respond to customers' compliance concerns, taking into account that well-articulated compliance readiness may offer a significant competitive advantage.