SCHWARTZ & BALLEN LLP
1990 M STREET, N.W. • SUITE 500
WASHINGTON, DC 20036-3465

WWW.SCHWARTZANDBALLEN.COM

TELEPHONE
(202) 776-0700

FACSIMILE
(202) 776-0720

MEMORANDUM

November 12, 2013

To Our Clients and Friends

Re: New Version of Payment Card Industry (PCI) Data Security Standards

The Payment Card Industry Security Standards Council has released an updated version of the Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standards (PA DSS). The PCI standards require merchants, processors, acquirers, issuers and service providers to implement specified protections for cardholder data and sensitive authentication data[1] that they process, transmit or store.

The new Version 3.0 standards will be effective January 1, 2014. However, Version 2.0 standards will remain in effect until December 31, 2014 to provide time for transitioning to the new standards. Certain new requirements have longer implementation timeframes.

Among other requirements, Version 3.0:

- Clarifies that sensitive authentication data cannot be stored after authorization, even if there is no primary account number (PAN) stored.

- Clarifies that all applications that process, transmit or store cardholder data are in scope for PCI DSS assessment, even if PA DSS is validated.

- Provides examples of how to determine the scope of the assessment and coverage of PCI DSS requirements.

- Clarifies the evidence that third parties must provide to customers in order for customers to verify the scope of the third party's PCI DSS assessment. Also clarifies the responsibilities of both the third party and their customers for scoping and coverage of PCI DSS requirements.

[1] Cardholder data includes primary account number (PAN) in combination with cardholder name, expiration date and/or service code. Sensitive authentication data includes full track data (magnetic stripe data or chip equivalent), CAV2/CVC2/CVV2/CID, and/or PINs/PIN blocks.

- Clarifies intent of the requirements to implement and maintain policies and procedures to manage service providers with which cardholder data is shared, or that could affect the security of cardholder data.

- Clarifies the applicable responsibilities for a service provider's written agreement/acknowledgement of PCI responsibilities.

- Requires entities to maintain information about which PCI DSS requirements are managed by each service provider and which are managed by the entity.

- Requires a service provider to provide written acknowledgment to its customers that it is responsible for security of cardholder data it possesses or processes, transmits or stores on behalf of customers or to the extent it could impact the security of the customer's cardholder data environment. (This requirement is effective July 1, 2015.)

- Establishes new technical requirements for payment application developers and vendors.

A link to the new PCI standards is available on our website at http://www.schwartzandballen.com/news.html

If you have any questions, please call Gilbert Schwartz, Robert Ballen, Tom Fox, Heidi Wicker, or Ben Gray at (202) 776-0700.