Payment Card Industry
Security Standards Council, LLC

401 Edgewater Place, Suite 600
Wakefield, MA 01880
Phone: 781 876 8855

PCI Security Standards Council update on PA-DSS and mobile payment acceptance applications
June 24, 2011

As part of its comprehensive examination of the mobile payment acceptance application landscape, in early 2011 the PCI Security Standards Council established a Mobile Working Group led by the Council's technical team and comprised of representatives from each payment card brand. Its purpose is to determine the need for advice, guidance or re-evaluation of existing PCI requirements for mobile payment transactions in the Council's specific areas of focus - the merchant, acquirer and processor acceptance space.

The working group has completed the first phase of this examination, focused on identifying and clarifying the risks associated with accepting payments via mobile solutions and validating mobile payment acceptance applications to version 2.0 of the Payment Application Data Security Standard (PA-DSS). During this evaluation, the working group determined that one of the major risk factors is the environment the mobile payment acceptance application operates within and the ability of such solutions to support the merchant in achieving PCI DSS compliance. Accordingly, the Council has classified mobile payment acceptance applications into three separate categories based on the type of underlying platform/environment and its ability to support PCI DSS compliance.

The categories are identified as:

- Mobile Payment Acceptance Application Category 1 – Payment application operates only on a PTS-approved mobile device

- Mobile Payment Acceptance Application Category 2 – Payment application meets all of the following criteria;
    i. payment application is only provided as a complete solution "bundled" with a specific mobile device by the vendor;
    ii. underlying mobile device is purpose built (by design or by constraint) with a single function of performing payment acceptance; and
    iii. payment application, when installed on the "bundled" mobile device [as assessed by the Payment Application Qualifed Security Assessor (PA-QSA) and explicitly documented in the payment application's Report on Validation (ROV)], provides an environment which allows the merchant to meet and maintain PCI DSS compliance

  "Bundled" solutions are defined as the validated payment application being provided to the customer together with specific version(s) of both the mobile device and the device's operating system/firmware.

- Mobile Payment Acceptance Application Category3 – Payment application operates on any consumer electronic handheld device (e.g., smart phone, tablet or PDA) that is not solely dedicated to payment acceptance for transaction processing

—more—

As a result of the working group's findings, mobile payment acceptance applications identified as Category 1 or Category 2 will now be considered for inclusion as PA-DSS validated payment applications.

Mobile payment acceptance applications identified as Category 3 will not be evaluated for PA-DSS validation until the development of appropriate advice, guidance and/or standards to ensure that such applications are capable of supporting a merchant in being PCI DSS compliant. This will be the focus of the next phase of the examination, in which the Council will collaborate with industry subject matter experts to produce additional guidance by the end of the year.

The Payment Application Data Security Standard addresses applications and systems used to store, process, or transmit cardholder data as part of authorization or settlement. At this time, guidance resulting from this examination will focus on the impact of these mobile solutions on merchant acceptance and processing channels.

***