Mobile Payment Acceptance Applications and PA-DSS *Frequently Asked Questions*

Purpose of document

The Council has completed the first phase of its examination of the mobile communications device and mobile payment acceptance application landscape, 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)*. The following has been compiled to address frequently asked questions around this topic.

Q What is the outcome of the first phase of the Council's examination of the communications device and mobile payment acceptance application landscape?

A *In performing this evaluation of payment applications designed for mobile communications devices, the Council determined one of the major risk factors is the environment the application operates within and the ability of that environment to support the merchant in achieving PCI DSS compliance. As a result, the Council has categorized mobile payment acceptance applications into three separate categories based on the type of underlying platform and its ability to support PCI DSS compliance, and has determined a clear direction for the next phase of the examination.*

Q What are the defined categories of mobile payment acceptance solutions?

A ***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 Qualified Security Assessor (PA-QSA) and explicitly documented in the payment application's Report on Valication (ROV), provides an environment which allows the merchant to meet and maintain PCI DSS compliance.

Note: "Bundled" solutions are defined as the approved 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 Category 3 – *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.*

Q What do these findings mean for the Council's current approach to reviewing mobile payment acceptance applications for PA-DSS validation?

A *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 that qualify as Category 3 will not be considered 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's PCI DSS compliance.

Q How will Category 3 applications that are submitted for validation be handled in the meantime? And what should vendors with Category 3 applications do in the interim?

A *There are many issues that need to be considered when determining whether or not a submitted payment application falls within the scope of the PA-DSS program. In all cases, mobile included, as soon as the Council can determine that a particular product will not be validated as a PA-DSS payment application, that submission is rejected.*

The PCI SSC recommends that mobile payment acceptance applications that fit into Category 3—and are thus not eligible for PA-DSS validation at this time but are intended for use in the cardholder data environment—are developed using PA-DSS as a baseline for protection of payment card data and in support of PCI DSS compliance.

Merchants and service providers using or wishing to use such applications in their cardholder data environment would need to include these applications as part of their annual PCI DSS assessment.

Q What criteria will be used to determine whether mobile payment acceptance applications that fit within Category 1 and Category 2 will be PA-DSS validated?

A *Should a PA-DSS candidate payment application seeking PA-DSS validation be identified as either a Category 1 or Category 2 solution (using the criteria stated above), that application will need to fulfill all PA-DSS requirements, as is the case with all payment applications seeking PA-DSS validation.*

Please see the PA-DSS Program Guide *for more information on the PA-DSS application submission process.*

Q What is the next step for evaluating Category 3 applications?

A *In the next phase of its examination, the Council will work across the industry to determine exactly how to address these applications, with the goal of delivering advice or guidance by the end of the year regarding the applicability of PCI requirements to Category 3 applications.*

Q What will be the process for listing mobile payment acceptance applications as PA-DSS validated?

A *For any payment applications that fit within either Category 1 or Category 2j and seek PA-DSS validation, vendors will follow the standard process for achieving PA-DSS validation by first working with a PA-QSA of their choice to have the product assessed against PA-DSS requirements, and then have that PA-QSA submit a Report on Validation (ROV) to the Council for review.*

Q When can PA-DSS validated mobile payment acceptance applications be listed?

A *Those mobile payment acceptance applications qualifying as Category 1 or Category 2 and seeking PA-DSS approval will be listed once it is established through the normal ROV review process that they meet all of the requirements of the PA-DSS 2.0.*

Q As a vendor, where can I go to find information on what's required for my mobile payment acceptance application to be validated?

A *The information provided in* the PCI Security Standards Council Update on PA-DSS and Mobile Payment Acceptance Applications *outlines what vendors need to know about the criteria for validation. Vendors can also take advantage of the* Which Applications are Eligible for PA-DSS Validation? A Guiding Checklist *that helps developers of all payment applications ask the right questions when determining which payment applications can be reviewed and validated by the*

Council as secure for accepting and processing cardholder data and support merchant PCI DSS efforts. For details about the PA-DSS application submission process, please see the PA-DSS Program Guide*.*

Q What does this mean for merchants and vendors?

A *Making use of mobile payment acceptance applications that fit within either Category 1 or Category 2 facilitates merchant and vendor efforts to comply with PCI Standards.*

Since Category 3 mobile payment acceptance applications are not eligible for PA-DSS validation at this time, entities wishing to use such solutions would need to make their own risk assessments around the use of such solutions in consultation with their acquirers and applicable payment brands. Such solutions would be included in an entity's annual PCI DSS assessment to ensure that the application and its operating environment are compliant with all applicable PCI DSS requirements.

Please note that each payment brand manages their own compliance validation programs, which may include conditions for use of non-PA-DSS validated applications, reporting requirements, due dates, fines and penalties, etc. For information about the individual payment brands' compliance requirements, please contact your acquirer (merchant bank) or the payment brands directly.

Q How will this affect those eager to deploy mobile payment acceptance applications that meet PCI requirements?

A *Use of PA-DSS validated Category 1 and Category 2 mobile payment acceptance applications provides assurance they are deploying payment applications into mobile environments that support their PCI DSS compliance efforts.*

Q Where do consumer-facing mobile payment acceptance applications and contactless technologies such as NFC fit into this classification?

A *It is important to distinguish between mobile payment applications used to initiate payments and those mobile payment applications used by merchants for payment card acceptance and processing. The PA-DSS program addresses payment applications used to accept and process payment for goods and services. Applications used for payment-initiation—for example, those downloaded by consumers onto their mobile phones and used for consumers' personal shopping—are seen as similar to the payment card in a consumer's wallet. The Council's purview does not currently extend to, nor is PA-DSS applicable to, consumer-facing mobile payment-initiation applications.*

Q What should merchants do while waiting on additional guidance from the Council?

A *In the interim, merchants should make their own risk assessments around the use of mobile payment solutions, considering the advice of their QSA and in consultation with their acquirers and applicable payment brands. The mobile payment acceptance application vendor may be able to help answer some key questions such as: whether the mobile payment application meets PCI requirements (for example, protecting the primary account number (PAN) throughout the transaction, including encryption over public networks, logging, and preventing malware attacks), and, if controls are in place in the payment application to support PCI DSS compliance, how this has been tested to demonstrate consistent use of those controls.*

Merchants should also be aware that any mobile devices and applications used in their cardholder data environments must be reviewed as part of their annual PCI DSS assessment. Merchants are also encouraged to refer to the PCI SSC website for a current list of PA-DSS validated applications.