Payment Card Industry
Security Standards Council, LLC

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

PCI Security Standards Council statement on policy for validated payment application security disclosure
April 6, 2012

As part of the Payment Application Data Security Standard (PA-DSS) program, the PCI Security Standards Council (Council) works diligently to maintain a listing of validated payment applications for merchants and vendors to use confidently in their payment environments. To help ensure the integrity of this list, the Council requires vendors that choose to participate in this program to disclose to the Council any vulnerabilities that could jeopardize the security of third party data.

Recent media reports have incorrectly cited "new changes" to the Council's disclosure policy for vendors participating in its PA-DSS Payment Application Validation program. To avoid any confusion, there have been no changes to the Council's policy since the PA-DSS program was launched, more than three years ago. The policy provides the Council with the requisite information and mechanism to act swiftly and appropriately when vulnerabilities are detected, thereby helping to ensure the security of application users and that applications identified on the Council's List of Validated Payment Applications meet Council security requirements.

As always, the Council encourages organizations to share feedback with the Council that may help evolve any aspects of its standards or assessment process for the good of the industry. Currently, we are in the formal feedback period for the next revisions of the PCI Data Security Standard (PCI DSS) and the PA-DSS. Participating Organizations and members of the PCI assessment community are invited to submit their input online:
https://www.pcisecuritystandards.org/pdfs/pr_20120327_PCI_Feedback_Period.pdf

***