

*PCI Security Standards Council Issues New
Payment Application Data Security Standard*

April 28, 2008

In our commitment to keep our Clients abreast of important issues and changes that may impact their compliance with one or more of the PCI standards, PSC is releasing this bulletin related to the announcement of the new PCI Payment Application Data Security Standard (“PA-DSS”) announcement by the PCI Security Standards Council (“PCI SSC”).

Background

On April 15, 2008 at the Electronic Transaction Association show in Las Vegas, Nevada, representatives from the PCI Security Standards Council announced the establishment of the PA-DSS. As of October 15, 2008, when protocols and procedures have been fully implemented, this new requirement will supersede the Visa USA Payment Application Best Practices (“PABP”). Any products certified to PABP will be grandfathered in for up to two years from qualification date.

The PA-DSS is an evolution from the original Visa USA PABP. The PABP was established by Visa USA as a best practice to be applied by software publishers to their payment application products. As attacks on applications continue, the evolution from a regional best practice to a global standard was anticipated. In PSC’s opinion, this will expand contribution to an important component of a merchant’s overall information security initiative. By implementing certified payment applications, merchants can rely on the level of security capabilities within an application to help reduce the likelihood of a catastrophic information security compromise.

Analysis

It is very early in the process to identify many details related to the new standard. PSC is preparing a complete analysis of the PA-DSS and comparison to the Visa PABP version 1.4. That said, the PCI SSC is still establishing protocols, procedures and training programs over the next coming months.

All Qualified Security Assessors wishing to perform PA-DSS assessments are required to go through “re-training” as soon as the PCI SSC have scheduled the training courses. We’re told the re-training will take place this July/August. Once re-training and certification is complete, PSC will be able to perform upgrade reviews and certification for any current Visa PABP to PA-DSS for our Clients.

Software publishers and companies that are in process or planning to get their applications certified should continue their PABP certification efforts.

The PCI Security Standards Council has made a clear statement that Visa USA will continue to review and accept PABP Reports on Validation until October 15, 2008. At that time the PABP list of certified applications will be transferred to the PCI Security Standards Council.

Products certified under PABP will be grandfathered onto the PCI Security Standards Council certified applications list for up to two years.

Going forward, the PCI Security Standards Council will take over the review and acceptance of Reports on Validation. All Reports of Validation submitted to the PCI Security Standards Council must be to the PA-DSS requirements. The Council will also take over maintenance of the list of certified applications, effective October 15, 2008.

From information we have, the PCI Security Standards Council may charge a listing fee per year per application for listing an application as “PABP compliant” or “PA-DSS compliant”.

More Information

This is an initial bulletin on the PA-DSS release. PSC will be releasing more information in the future.

To get more information and help, contact PSC at 408-228-0961 x 104 or contact your PSC QSA directly.