## Updated PCI Standards: Flexibility, Clarity and Common Sense 2.0

The Payment Card Industry Data Security Standards (PCI DSS) are a set of 12 requirements that merchants and their business partners are expected to follow to ensure the safety of cardholder data. Authored by the PCI Security Standards Council—an independent consortium of representatives from the major credit card brands—the PCI DSS covers data management, information technology, encryption, physical security, legal agreements, and business operations. When these standards were updated from version 1.1 to version 1.2, 30 changes were introduced to the existing requirements.

By the time you read this, the effective start date of the new standard, October 1, 2008, and the sunset date of the old standard, December 31, 2008, will have long passed. While assessments started prior to October 1, 2008 can be completed according to V1.1 and assessments started between October 1, 2008 and December 31 can use either version, it's worth noting that complying with the new standards now may actually be easier than reexamining your processes down the road.

PCI 1.2 is intended to reduce confusion and, in some cases, grant leeway around requirements that were deemed unduly burdensome. Some of these "flexibility" changes—like allowing for a risk-based approach to applying patches, as defined under Requirement 6—may sound like a huge gain for large organizations with complicated networks. However, it's been our experience that companies that have difficulty patching within a 30-day timeframe will have an equally tough time determining risk levels and conducting regression testing on critical systems.

Requirement 9 also introduces two notable changes: one of which is the addition of a mandatory, annual site visit to off-site storage facilities. Given that many of the major storage vendors are not prepared to accommodate such visits, this could cause some pain. However, the added flexibility in choice of datacenter access controls, which previously had to include cameras, is helpful to small companies that don't keep their servers in a typical datacenter.

Other updates seek to clarify and strengthen the PCI DSS. An example of this can be found in Requirement 5, which previously contained a note stating UNIX-based systems and mainframes were typically not affected by viruses. This note has been removed, so now it is clear that merchants using UNIX systems also are required to protect any system that is potentially at risk to malicious attacks.

Requirement 11 now mandates internal and external penetration testing. While the rules specify that your internal team can do this work, it's never a bad idea to bring in an external assessor to verify your methodology. You don't have to pay a Qualified Security Assessor (QSA) to conduct all your testing; you can limit the engagement to a review of your results and test procedures. View this extra help as a training opportunity for your staff and a chance to identify your strengths and weaknesses before a breach occurs.

Some of this "toughening" may seem difficult to enforce, and the inclusion of removable media (iPods, PDAs) to the list of employee-facing technologies referenced in Requirement

12 is one such example. Yet, here is a case where there are a number of simple solutions at your fingertips. Use a BIOS-level control to disable USB ports or remove them from your workstations and lock the case so your employees cannot modify the hardware or reset the BIOS. Reinforce these measures by adding language to your employee handbook that prohibits the transfer of data to peripheral devices.

Applying a little “Common Sense 2.0” will tell you to look for the low-hanging fruit before you spend big dollars on expensive security measures. The key to security is utilizing multiple layers of process to minimize the potential for risk and loss. Sometimes security controls require more than a single tool to be effective.

Understanding how PCI changes affect compliance certification and security practices is critical to avoiding costly mistakes. Teams charged with PCI compliance work should be wary of assuming that greater flexibility means less security when, in fact, it usually means the opposite.