



**PCI DSS CREDIT CARD SECURITY STANDARDS
PA DSS PAYMENT APPLICATION STANDARDS
BEST PRACTICES BECOME MANDATES 10/01/2009**

Just when you thought PCI was easy -- There's a major PCI-related deadline coming up on October 1st, and most merchants aren't aware of the details, even though they've been given an entire year to get up to speed. It is known as "Phase III" of the PA DSS compliance mandates, and it is the first major push to get Level 3 and 4 merchants to wake up to the importance of PCI. **Like other PCI related mandates, it's driven by Visa, through the card acquirers, and it requires that the acquirers not board (sign up) any new merchants that are not EITHER PCI compliant OR running PA DSS compliant payment applications.** This is designed to stop merchants from switching from "tough" to "easy" acquirers, among other objectives. But, what's interesting is that only last year these were Visa's "best practices," for merchants and vendors, and they are now becoming the toughest and most comprehensive of the standards designed to secure the payment process.

When best practices become mandates -- There's a big difference, in general, between best practices and mandates. The study of PCI Best Practices that the PCI Knowledge Base is doing for the National Retail Federation would be very different if they were all mandates -- and we'd get a lot of merchants pretty ticked off. Well, that's the sort of impact we're expecting among the merchant community as the Payment Application Best Practices (PABP) become powerful mandates in 2009 and 2010. **The power of PA DSS is contained in just a couple of sentences: As of October 1, 2009, the payment networks and their agents must "de-certify" vulnerable (non-compliant) payment applications and on July 1, 2010, non-compliant payment applications will no longer be processed by the payment networks. Get it? Transactions from non-compliant application won't be processed. Period.**

All merchants, listen up -- This is not a mandate just for Level 1 merchants; it applies to all merchants, everywhere. Now, I'm not a betting man (anymore -- long story), but I'm willing to bet that about 99 percent of merchants haven't thought this through and started making plans to change out (or upgrade) their software, which will involve much more than creating a bunch of reports for the PCI assessor's annual visit. It turns out that when you upgrade or switch your payment applications, a bunch of other applications may not work so well. Even though the deadlines are a year or two away, when you add in the PED device deadlines (don't get me started on those), merchants simply cannot wait to plan the upgrade for another six months.

Getting on the “white list” – One of the biggest differences between PCI DSS and PA DSS is that while there’s no list of PCI compliant merchants, there is a list of PA DSS compliant vendors and products. Actually, there’s a list of PABP-compliant vendors and products that is being upgraded during this “transition period” to be a list of PA DSS vendors and products. The object is to provide a list to make it easier for merchants to select compliant products. That’s handy. We love lists. However, by creating such a list, Visa (now the PCI SSC) has provided a HUGE incentive to vendors to get on that list, since it can affect company revenues by millions of dollars, more or less. Add to this that the PCI (and PA DSS) assessment market has become very price-competitive and the potential to “cut corners” in the name of cost effectiveness is growing, and will continue to grow substantially as these new “make or break” PA DSS deadlines approach. To combat this, the PCI SSC has put into place a new quality assurance (QA) process. That’s also good. We love quality. But then again, who is going to report “questionable” assessments of the vendors, when neither of the parties to the process (the vendor or the assessor) have any motivation to do so? That’s where the merchants come in: Merchants simply cannot assume that just because a payment application product is on some long list that there has been a thorough and complete review, comparable to a Level 1 merchant’s PCI DSS assessment. Merchants must review the detailed audit reports and even be directly involved in their vendor’s PA DSS assessment. Merchants must own this process, simply because they own the resulting liability and brand damage.

Payment outsourcing saves the day? – Several weeks ago, we wrote a column on why and how payment outsourcing will become a huge opportunity. This column is a partial explanation of why we take that position. Currently this is only common among Level 4 merchants, but the PA DSS mandates will, we argue, drive interest in payment application outsourcing among Level 3 merchants. On the other hand, the pricing of these services is a common source of complaints in our PCI Best Practices research. We expect that as the popularity grows, the average transaction fees will be reduced significantly due to competition. The question for many merchants is when is the right time, if any, to consider outsourcing to minimize both transition costs and transaction fees. We will be addressing this issue in a future column.

By the way, if you're a retailer, we want to get you involved in the best practices study we're doing for the National Retail Federation. If you'd like to participate, send me an E-mail at David.Taylor@KnowPCI.com .