Consumer Reality Check - Lifting the Veil on PCI DSS

I read an article entitled "Global Payments has some explaining to do" (Source: CSO) today and there were some interesting points made by Bill Brenner, managing editor of CSO. He asked specifically, "How on Earth were they designated PCI compliant in the first place? What were the specific actions they took to improve security and how did they allow those safeguards to fail? How rigorous was the auditing process? Did the QSAs put the processor through the wringer, or did they just casually saunter in, check off some boxes and move on to the next customer?"

These are great questions from a consumer standpoint. Being an executive insider, I'll share some insights and experiences that will lift the veil on the reality of the Payment Card Industries Data Security Standards. Nothing I am writing about is specifically citing any company directly. This is purely consumer revelation about the true nature of what PCI DSS really means.

In my career to date, I've been the Chief Security Officer and Auditor to several organizations within the banking, payment processing and retail markets all of which are subject to the PCI DSS guidelines. PCI for the layperson is simply a set of guidelines established by the credit card companies, specifically, Visa, MasterCard, American Express, Discover and JCB International. PCI is not driven, monitored, influenced or managed by the government, but by the same industry foxes guarding the proverbial henhouse.

Merchants and payment processing companies who process more than 6 million credit card transactions annually must independently hire qualified security assessors, otherwise known as QSAs. This independent business relationship between the buyer of required services and the seller of those services establishes the potential for collusion and fraud which I have seen in action first hand. The PCI certification is only as good as the honesty, integrity, and competence of the QSA which in my experience is extremely subjective. I can also tell you with a straight face that I've never worked with a QSA who didn't miss something crucial in their examinations, yet the client company receives a clean bill of health. Most of these client companies are trying to do the best they can; after all, it is their business and reputation on the line.

PCI is not a progressive standard. In the standard, it is acceptable to utilize antiquated encryption that was defeated ten years ago. The only reason for that is because banks would need to update their systems like ATM's which is expensive so we pull the teeth out of PCI for the sake of business convenience and not consumer protections. It's not the first time we have heard that one is it? Another nugget is I had mentioned that QSAs look at companies with six million annual card transactions. If your company processes one card less than six million, you only have to perform self-assessments. How many companies fall into this category you might

ask? Most companies fall into this category. Again, it's the same industry foxes guarding the proverbial henhouse here. PCI DSS is consumer eye candy.

In my opinion, QSAs should be regulated since they are the gatekeepers to credit card processing security for everyone. PCI should have government oversight since credit card processing requires consumer confidence and also because industries should not be allowed to regulate themselves. How many times will we as consumers see that scenario play out while we are ultimately left holding the bag?

Article first published as Consumer Reality Check - Lifting the Veil on PCI DSS on Technorati.