

the money guy

RISING SECURITY STANDARDS

RISING COST OF PROCESSING

(For Someone)

by Harold Montgomery



Perhaps you caught a press release in May about the need for web merchants and their processing service providers to install a web application firewall between their “web server” and end-point devices. This new firewall requirement is in addition to already existing firewall requirements. In addition, this standard requires a manual or automated security review.

The PCI Security Standards Council issued this new standard, called 6.6, which went into effect in June 30, about 60 days after it was issued. Providers had to scramble to adjust in that time frame or risk being out of compliance, and therefore legally liable for damages that might result from being vulnerable.

This isn't really a big change, but that's also not the point. Here's a Council, chartered by the card associations with a specific and important mission: Protecting consumer information. No one is going to argue with that. So, this Council is here to stay, and their charter won't change – in fact it will grow, they always do. The Council will gradually pursue new ways of protecting consumer information over time.

Councils like this don't fade away, they perpetuate themselves endlessly. They establish a professional community around themselves. They create means of communication (did you know there's a magazine called “Security Professional”?) They have awards and trade associations, and banquets and on and on. In short, this Council and its work now a permanent feature of the payments landscape.

And that's OK. We all need the processing system to be safe, and more importantly, to be seen as safe by all parties using it. What good would it be if any one participant in the system (consumers, banks, merchants or processors) believed that the system was not safe? The whole thing would break down - fast. So that's no good. We all have to do whatever it takes to make the system unquestionably safe. Period. No more TJ Maxx's. No more Card Systems.

But what's the cost of all this security and, and who bears it? Has anyone done a cost/benefit analysis on the

recommended changes? Was the lack of this new proposed firewall really a big issue with huge consequences to the system? Who's looking out for the processor/ISO/merchant side of this equation when it comes to the cost of implementation and support over time?

In short, no one – at least not that I can identify. The Council issues security standards and expects them to be followed. Their charter is to make things safe, not to make them cheap. Card Associations follow up with enforcement measures for those who don't comply and as a last resort, the legal system provides a method for damaged parties to pursue claims against those who were not up to accepted industry standards. You might ask, accepted by whom? The old adage that acquiring is the tail on the issuing dog is no more appropriately applied than in this case. While the benefits of security accrue to all parties, the acquiring side bears the cost of implementation and support disproportionately.

It takes people, resources and time to follow through with these standards, and those who have to keep up don't control the costs of doing so. Cost of compliance is a new cost element in our business and one that's not only permanent, but growing over time. You can expect these standards to rise over time, becoming more complex and therefore more expensive to implement. Plus, they have to be consistently monitored and maintained. Thieves are becoming more clever and the security professionals charged with stopping them are constantly racing to keep pace. There's really no way to make our systems totally safe from hackers, but that won't stop the industry from trying.

All this is good news for software engineers and consultants, but it means rising and unpredictable costs for processors and indeed anyone who is on the receiving end of a new standard. That includes anyone in the chain of delivery of processing services – processors, software vendors, merchants and ISOs who are expected to educate merchants about security protocols.

Nowhere is this issue more obvious or painful for the acquiring community than when it comes to the implementation of EMV standards for POS equipment. Here is a great example of uneven costs and benefits. EMV as implemented in Europe required that all retailers change their terminals to chip-and-pin technology to reduce fraud on the issuing side. EMV makes it almost impossible to counterfeit cards. It certainly had the desired effect, benefiting the issuing side by reducing fraud by over 30% in two years, about 10 basis points.

Think of EMV as the final, best solution for card fraud. The problem is that the costs of implementation largely fall on the acquiring side of the business and the benefits fall on the issuing side. This is one of those situations where what may be good for the industry is bad for a few of its constituents. But in the bigger picture, if data breaches don't stop, the industry may have to adopt tighter mandated security standards. It's easy to see Congress forcing an air-tight approach to security to satisfy a scared public, if the industry doesn't solve the problem on its own. With that thought in mind, EMV may make sense as a preemptive move designed to avoid a greater level of regulation and government oversight.

There's more and more talk about security and less and less talk about what it costs. There's no such a thing as perfect security out there, and we will never achieve it. It seems to me that a certain amount of fraud is tolerable and sustainable. We can keep it at a reasonable level with a reasonable investment. Or we can chase perfection and drive costs out of control. I hope someone on the Council is thinking about the dollars. ■

Harold Montgomery is the CEO of Calpian, Inc., a Dallas, Texas-based provider of financing opportunities to all levels of merchant acquirers. Montgomery submitted expert testimony to Congress regarding Acquiring Industry Legislation. You can contact Harold at 800.589.1173 or portfolio@calpian.com.

