October 2, 2007

Mr. Bob Russo
PCI Security Standards Council, LLC
401 Edgewater Place
Suite 600
Wakefield, MA 01880

Dear Bob:

We have appreciated the opportunity to work with the credit card industry on data security matters over the past several years. Reducing credit card fraud is a goal both of our industries want to achieve.

Toward this goal, the retail industry is investing hundreds of millions of dollars annually in systems and procedures to better protect credit card data. Much of this spending has gone toward making retailers compliant with the standards put forth by the Payment Card Industry Security Standards Council. Among the largest retailers who process the greatest volumes of credit card transactions, 40 percent have been certified as compliant with the Payment Card Industry (PCI) Data Security Standard, and an additional 50 percent have submitted their initial validation or are otherwise on the road to achieving compliance.

While those achievements are notable, they are not enough to accomplish the ultimate goal of protecting the consumer. Data breaches have continued to occur at an unacceptable rate. There have been numerous instances of hackers targeting sophisticated retail computer systems that store or process credit card data, stealing the data and then using it to commit fraud.

PCI, which has been in existence in one form or another for several years, was supposed to prevent such crimes. It is a valiant attempt to prevent large stockpiles of credit card data from getting into the wrong hands. However, it is unlikely PCI will ever be able to keep pace with the continually-evolving sophistication of the professional hacker, or anticipate every possible variation of future attacks. We believe the time has come to rethink the assumptions behind PCI.

Much has been said about PCI being a moving target, and how retailers have been forced to jump through extraordinary hoops in the quest to achieve compliance. We don't want to reiterate those arguments here. But a primary reason that PCI exists and retailers have been forced to jump through those hoops is because credit card company rules require merchants to store the credit card data that criminals are so eager to steal.

Let me be clear. All of us -- merchants, banks, credit card companies and our customers -- want to eliminate credit card fraud. But if the goal is to make credit card data less vulnerable, the ultimate solution is to stop requiring merchants to store card data in the first place.

Rather than requiring that merchants keep reams of data -- currently required under card company rules in order to satisfy card company retrieval requests -- credit card companies and their banks should provide merchants with the option of keeping nothing more than the authorization code provided at the time of sale and a truncated receipt. The authorization code would provide proof that a valid transaction had taken place and been approved by the credit card company, and the sales receipt would provide validation for returns or proof of purchase. Neither would contain the full account number, and would therefore be of no value to a potential thief. Any inquiries about a credit transaction would be between the cardholder and the card-issuing bank.

If all merchants took advantage of this option, credit card companies and their member banks would be the only ones with large caches of data on hand, and could keep and protect their card numbers in whatever manner they wished. The bottom line is that it makes more sense for credit card companies to protect their data from thieves by keeping it in a relatively few secure locations than to expect millions of merchants scattered across the nation to lock up their data for them.

We believe this is the most effective and efficient approach to protecting credit card data and preventing a continuation of the data breaches that have been seen in recent years. If the PCI Security Standards Council is willing to solve this problem, NRF and its members stand ready to work with you to help you protect the nation's consumers from the growing threat of credit card fraud.

Sincerely,

David Hogan
SVP and CIO