



Dr. David Taylor, CISSP

Founder

PCI Knowledge Base

CREDIT CARD SECURITY

Why Not Implement Tokenization to Replace Card Data?

Despite how attractive tokenization sounds as a concept, there is substantial resistance to the products and services.

As we were collecting over 100 hours of interviews with merchants, banks, card processors and PCI assessors for the PCI Knowledge Base, we were surprised at how many merchants were outright resistant to the technology. The deployment of tokenization technology replaces credit card numbers with surrogate numbers, in order to reduce the scope of a PCI audit and reduce risk by reducing the number of places where card data is retained. The interviewees offered a number of explanations for this resistance. Some of the most prominent are listed here.

Companies Have Already Spent Money on Encryption

The most popular reason for not implementing tokenization is that companies have already implemented data encryption and key management systems costing hundreds of thousands of dollars, and they did not feel they either needed tokenization, or they were unwilling to be perceived by upper management as “changing course” by recommending they remove the data they just spent all this money to protect.

Applications Managers Won't Give up the Data

A near rival for the top reason for resisting tokenization is that business managers and application owners use card numbers in many different places in their business processes and applications, and that the security managers, who typically prefer tokenization (as it reduces their own risks), do not believe they can successfully argue that the applications could be rewritten to work with the token numbers instead. They feel that the costs for changing the application code cannot be justified by the level of risk reduction.

Merchants Are Waiting for Their Bank or Database Vendor

Some of the merchants said they would be willing to consider tokenization, but not from the current crop of smaller, independent vendors. Some said they

felt such solutions would soon be offered by their own bank or card processor, others (typically in IT) said they wanted to wait until tokenization is an option built into their DB management software.

Tokenization Is Too New or Unproven

Some of the merchants who resist using token numbers as substitutes for card data are simply objecting to the fact that there are not enough reference accounts who are willing to talk about their experiences. Very few companies want to be first to take what they perceive as an additional risk relative to their credit card data, so they want to be assured their peers are involved. The fact that this becomes a self-fulfilling prophecy is clearly not lost on these merchants.

Tokenization Vendor Is a Single Point of Failure

Some of the merchants and PCI assessors interviewed expressed concern that by having the card data from hundreds, even thousands of companies concentrated in one place (a tokenization vendor's systems) that this could make the vendor such an attractive target (like the Department of Defense or National Security Agency), that so many talented crackers would be pointed at the repository. With that, they reason, “someone” would break down the defenses. This treasure trove of data would be equally attractive to privileged insiders, thus making a detailed review of any tokenization vendor's solution absolutely mandatory.

Tokenization Pricing Models Are Immature and Too Variable

We spoke with a few merchants who had done head-to-head comparisons among the major tokenization vendors, and they encountered highly flexible pricing models. A larger concern was that the merchants had no idea how to tell if they were getting a good deal, as the pricing models were difficult to compare across vendors.

The Bottom Line

Despite how attractive tokenization sounds as a concept, there is substantial resistance to the products and services as they exist in the marketplace today, sufficient to limit the growth of this market in the next few years.