5 Myths of Encrypting and Tokenizing Sensitive Cardholder Data

By David Kilgallon, *Director of Integration Services at CardConnect*

Payment security is complex, with risks and vulnerabilities present at every point of the processing chain. As hackers develop increasingly sophisticated methods to exploit the weak points of a business's payment system, it's no wonder why data breaches have spiked in recent years.

In 2012, there were at least 682 breaches resulting in the theft of nearly 28 million consumer records, the highest number of successful attacks ever recorded by the Privacy Rights Clearinghouse. And the information that cybercriminals sought most, according to Trustwave, was cardholder data – the information contained on a consumer's payment card, embedded either in a magnetic stripe or chip.

Although not yet mandated by the PCI SSC, there are two solutions that, when combined, are widely considered the best way to protect against data theft: encryption and tokenization.

Encryption, where plain-text card data is converted into ciphertext, and tokenization, where sensitive payment data is replaced with a unique identifier known as a token, render cardholder data unreadable – and thus meaningless – to unauthorized third parties such as hackers.

While implementing encryption and tokenization can safeguard against weaknesses in the payments process, thereby reducing a merchant's PCI scope and compliance costs, there still are five misperceptions about these solutions.

Myth #1: If my data is encrypted, it can't be stolen.

No security solution will protect sensitive data completely. With constantly emerging threats carried out by increasingly intelligent hackers, companies should operate under the assumption that their data will be compromised at some point. What encryption and tokenization can do is soften the blow, should a breach occur; cyber thieves cannot decrypt or read stolen card data without a key, and tokens stored in a secure vault essentially are meaningless to anyone but the merchant and its payment processor.

It's important to note that different levels of security can be obtained through a combination of different types of encryption and tokenization. Session-level encryption transmits unencrypted card data through an encrypted transaction tunnel, while data-level encryption applies to the actual card data within the tunnel. There are multiple approaches to tokenization, too.

Make sure the vault storing data is protected by strong security – by encrypting data placed in the vault, backing up copies of the database encrypted, tightly controlling physical and virtual access to the server that hosts the database, and placing strong user authentication for anyone trying to access the server.

Myth #2: Encryption and tokenization are too complicated to implement, especially at the enterprise level.

Encrypting and tokenizing data is a complicated process. But the technicalities should be left to a trusted payment partner who can lessen the IT burden. Merchants should be offered a customized solution that meets their unique data protection needs, along with a well-designed management console to help them control the system once it's in place.

To ease the effort, look for a service partner that has coded to standard payment system specifications, e.g., those already published by your ERP application company. Many large ERP applications already allow for easier integration by publishing an application programming interface (API) for interacting with payment gateways.

Secondly, if available, find a service partner that has their own published APIs to allow you to integrate directly to the services they provide. For smaller merchants with smaller IT departments, this may be the case since nobody knows your POS application better than you.

Next, look for services, support and features that make the development AND ongoing maintenance easier from a business and IT perspective. These might include sample code, test cases, debugging tools, documentation, reporting portals and the ability to monitor transactions in real-time.

Finally, take advantage of some cutting edge tools by partnering with a company that is "ahead of the curve" with regard to processing technology. Some examples include offerings and support for mobile apps, EMV, virtual terminals and any of the other latest trends. Adopting new processes that are faster and more efficient will help your business operate at a higher level.

Myth #3: Encryption and tokenization are too expensive.

The financial repercussions of a data breach can easily dwarf the upfront expense of putting encryption and tokenization in place.

The process of implementing both solutions will give merchants a comprehensive understanding of where their sensitive data resides. This will prompt a project to reduce the number of places where such data is stored, leading to less necessary protection points and thus better security.

Put simply, using encryption and tokenization in back-end business applications leads to less data scattered around the enterprise environment that is subject to PCI compliance audits. Both solutions reduce the investment needed in data protection costs over the long term, and they lower merchants' PCI scope; by eliminating actual cardholder data from the system, the likelihood that a breach will occur reduces, and thus so does the time and cost of PCI validation.

Myth #4: Any information, if encrypted, can be stored on my network.

Many merchants have a legitimate business reason for storing cardholder data, but it's important to understand exactly what pieces PCI standards allow them to store and which ones are off limits.

Even if encrypted, some sensitive data – such as the information contained in a cardholder's magnetic stripe or chip, card security code (CVV) and PIN – is unauthorized by the PCI SSC, and therefore may never be stored after payment authorization. Only the primary account number (PAN), expiration date, service code or cardholder name can be stored.

Myth #5: Only businesses subject to PCI compliance benefit from encryption and tokenization

A business is subject to PCI only if it accepts credit, debit or pre-paid cards as payment for goods or services. However, there is a good chance that all businesses process sensitive payment information on behalf of employees, as well as digitally store customers' personally identifiable information (PII). In both of these instances, the same tokenization and encryption that helps with PCI can be applied to PII.

With cyber-attacks increasing and legislation on PII security becoming more prevalent, the obligation of businesses to safeguard customer and employee data has become a fiery issue. Rather than stall to protect PII until it is a legal obligation, businesses should act swiftly to encrypt and tokenize all personally identifiable information.

I hope deconstructing these myths helped your understanding of encryption and tokenization, and why safeguarding sensitive information is so important.

*For more helpful articles about the ins and outs of the payments industry, visit **cardconnect.com/blog**.*