CREDIT CARD SECURITY

The Best Way to Secure Data Is Not to Store Data

JD Oder
Founder, CTO
Shift4

Credit card data theft is a serious threat to any business. Should a breach occur, companies suffer major damage to their brand image and to their bottom line, not to mention the fines involved if the merchant is out of PCI compliance at the time of the breach. In addition to financial loss, there is also a relationship between credit card data theft and our National Security. The FBI and the Department of Homeland Security have recently reported credit card data theft as a growing source of revenue for terrorist groups.

The increase in breaches has been accompanied by a corresponding shift away from payment processors with large amounts of credit card data to hotels, restaurants and other companies in the hospitality, travel and entertainment industries. The reason for this shift is driven by the thief's ultimate objective which is to obtain magnetic stripe data in order to create counterfeit cards which can be used or sold on the black market. Another reason these market segments are more attractive targets is because the cards carry higher credit limits and are less likely to have fraud reported by the user. Cards issued to frequent business travelers fit this description. Additionally, hotels and restaurants tend to store more information in order to facilitate tips, late fees and similar associated charges.

Securing credit card data and preventing its unauthorized use, while also preserving the payment processing systems now in use by millions of merchants, is a vital concern for consumers, government and businesses. New technologies exist today that replace real credit card data with an electronic token. The primary objective of tokenization technology is to enable businesses to operate normally while not storing sensitive card data in their systems. Payment applications built on tokenization can be used on existing legacy systems so merchants do not need to buy new equipment in order to become truly secure.

What Is Tokenization?

The basics of tokenization are straightforward. A transaction is swiped as usual at a POS or PMS terminal. Once transmitted to the processor for authorization, the data is converted into a token which is a globally unique, randomized representation of the real card number. After receiving the authorization from the processor, only the token is sent to the customer while the authorization response and the real card number is held in a secure data center. The merchant no longer has the burden of storing or protecting the cardholder number. The token spans the lifetime of the transaction, so it provides all of the same support for tips, tabs, incremental authorizations and chargebacks as a stored card number would.

PCI Standards Reinforcement

Tokenization reinforces the overall objectives of PCI standards as well as specific requirements. First and foremost, PCI requirement No. 3: Protect stored data. By returning only tokens in response to merchant requests, there is no cardholder data stored on the merchant system. Merchants no longer have to deal with complex encryption methods and since the merchant is not required to encrypt the token, there are no encryption keys to manage. Tokenization also meets PCI requirement 3.4 which mandates that cardholder data be rendered unreadable using one of several forms of strong encryption. One of the methods suggested is truncation. Since only the last four digits of the card number are used in the token, this requirement is met. Further, since the merchant is not using encryption to derive the token, requirements No. 3.5 and No. 3.6 are moot.

Tokenization provides merchants with the ability to eliminate much of the sensitive data that is usually stored, thereby supporting the objectives of PCI and also achieving real security. Merchants are being targeted more frequently than ever and with greater success. In addition to the financial and brand damage that follow a breach, current state and federal legislation exposes merchants to additional financial and legal liability if they are breached and card data is stolen. Staying one step ahead of the latest attack methods is a challenge for even the most security-minded companies. Those without the internal expertise to guard against the onslaught of data thieves are indeed gambling with their company's assets. Recent headlines suggest this is not a good bet. "They can't steal what you don't have."

Thieves can't steal what you don't have.