APRIL 2011

Bank of America
Merchant Services

How security can help grow your business: the marketing side of tokenization

First Data Market Insight

EXECUTIVE SUMMARY

In recent years, tokenization and encryption have become two of the leading technologies for the protection of sensitive payment card data. In fact, tokenization has become such an important means for merchants to protect data post-authorization that the Payment Card Industry (PCI) Security Standards Council (SSC) is considering whether tokenization should be included in an upcoming version of the PCI Data Security Standards (DSS).[1]

TABLE OF CONTENTS

[1] Digital Transactions, "Encryption, Tokenization Loom Large As PCI Council Mulls Changes," October 7, 2009

Many merchants are not waiting for tokenization to be mandated; they are using the technology now to vastly reduce the risk of a data breach as well as the scope and cost of their PCI security audits. But along with the security benefits, these companies have discovered an additional business advantage. Tokenized payment data opens up numerous possibilities, especially for those companies that have not previously kept transaction data after the authorization and settlement processes.

What kind of possibilities? Non-sensitive tokenized data can be used in back-end business operations to develop innovative marketing campaigns, create customer loyalty programs, conduct business data analysis, and even assist with loss prevention. These types of value-add applications enhance the overall business case for a merchant to implement a tokenization solution. By substituting tokens for Primary Account Numbers (PANs), the merchant is now able to perform new functions without risking the exposure of real cardholder data.

Non-sensitive tokenized data can be used in back-end business operations to develop innovative marketing campaigns, create customer loyalty programs, conduct business data analysis, and even assist with loss prevention.

CREATE NEW BUSINESS OPPORTUNITIES

The best way to visualize this kind of new business opportunity is with an example. Consider the case of a quick-service restaurant (QSR). The business accepts credit and debit cards from its customers, who typically make purchases in amounts less than $25.

In the old business model, the restaurant does not keep information related to the payment cards beyond the settlement process because there is little need to retain this data in a QSR business. If the restaurant must handle a chargeback or return — a relatively uncommon occurrence for QSRs — the transaction is completed in cash. Unfortunately, in this traditional model there is no method for tracking or analyzing a customer’s behavior over time, because nothing has been captured to act as a reference to associate transactions with that customer. Once the customer receives his food and walks or drives away from the point-of-sale (POS), the opportunity to learn more about his habits and preferences is gone.

In the new business model — one in which the QSR receives tokenized data from its payments processor after authorization — there is now a permanent and safe reference number to tie back to that specific customer. The QSR can analyze the transaction data to understand more about the customer, such as which location(s) he dines at, what time of day he frequents the business, what he purchases, and so on.

The company could turn information about customer buying behavior into targeted POS promotions, such as a discount coupon for a future visit printed on the sales receipt after the customer has visited the restaurant “x” number of times. Or, the data could be used to support a loyalty rewards program for frequent customers without having to issue a separate loyalty card. The advantage here is that loyalty programs increase annual same store sales an average of 4 percent.[2] This is not surprising; when given a choice between a restaurant with a loyalty program and one without, more than 60 percent of consumers will choose the restaurant with the loyalty program.[3]

A PRIMER ON TOKENIZED DATA

Now that we have established that operational processes enabled by tokenization can help grow a business, it may be helpful to provide a more detailed explanation of tokenization. What is it? Who manages the process? How does it fit into a company's business operations?

In general terms, tokenization is the process of creating a string of random characters called a token (or alias) that acts as a substitute for real data. Often, the original data is too sensitive or valuable to thieves to be maintained for analysis as-is. The data could be cardholder account numbers, personal health information, social security numbers, or a variety of other types of information that must be protected from possible exposure or theft.

> In general terms, tokenization is the process of creating a string of random characters called a token (or alias) that acts as a substitute for real data.

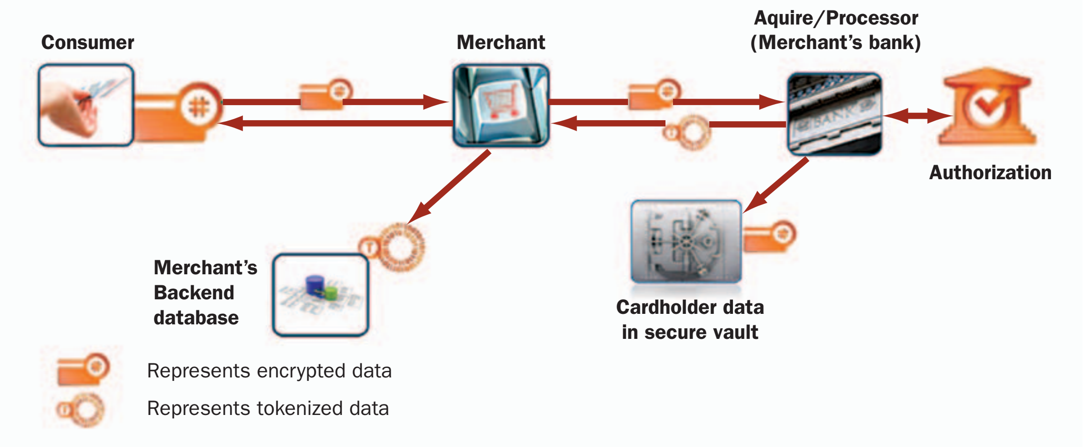
In the merchant world, the sensitive data is usually the account number associated with a customer's payment card. The process of tokenizing this data is often built into the payment authorization process and managed by the merchant's acquirer or processor. When using a service-based tokenization model, there is no equipment for the merchant to buy or install. When a payment card is used in a transaction, the authorization takes place as usual. Once authorized, the actual PAN is sent to a centralized and highly secure server called a "vault" where it is stored by the payment processor. An index table in the vault creates a permanent relationship between either the card number or the transaction number and a token. Immediately after the PAN is tokenized, the desensitized substitute number (token) is returned to the merchant's systems for use in place of the PAN, which is no longer needed after authorization. The process is shown on the next page in Figure 1. The end result is that the token can be used in various business applications as a safe and reliable substitute for the real PAN.

[2] Chockstone, Inc., http://www.chockstone.com/products/loyalty

[3] Chockstone, Inc., http://www.chockstone.com/markets/restaurants

TOKENIZATION IS NOT THE SAME THING AS ENCRYPTION

Figure 1: Tokenizing data as part of the payments process

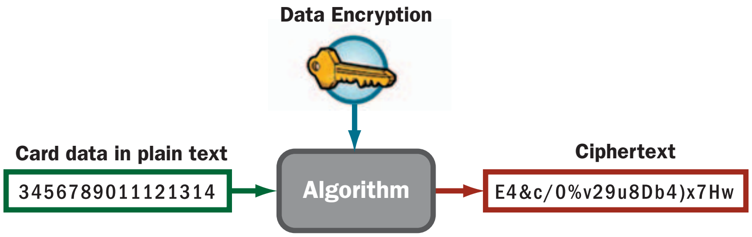

Consumer
Merchant
Aquire/Processor (Merchant's bank)
Authorization
Merchant's Backend database
Cardholder data in secure vault
Represents encrypted data
Represents tokenized data

On the surface this may sound like encryption, but it is not; there is an important difference between encrypted numbers and tokenized numbers.

Encryption involves the application of a mathematical process to the data to render it unintelligible or unusable. Encryption is distinguished by being repeatable, reversible, or both. There is a direct mathematical relationship between the original and the derived value, called ciphertext. Although secure, it is possible to regenerate the original value if someone has the "key"—the algorithm that reverses the encryption process. Therefore, it is very important to protect the key that can decrypt the data. Key management can be quite a complex process. The data encryption process is illustrated in Figure 2 below.

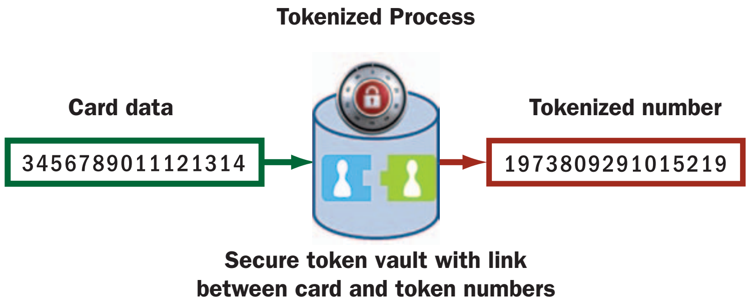
Encryption involves the application of a mathematical process to the data to render it unintelligible or unusable. Encryption is distinguished by being repeatable, reversible, or both.

Figure 2: The data encryption process



In contrast, the association between a token number and the original value is maintained in an index database (the vault), and there is no direct mathematical relationship between the original value and the resulting token. There is no key that can reverse the process to turn the token back into meaningful data. A token is simply a random string of characters. The only way to regenerate the original data from the token is to reach into the highly secured vault and use the index to relate the token to the card data. This is virtually impossible for thieves to do. See figure 3 below for an illustration.

Figure 3: The Tokenization process



Technically speaking, encrypted numbers could work as substitute values for real card numbers in backend business applications. However, key maintenance and the process of encrypting and decrypting the data would be so cumbersome as to make the applications impractical. What's more, using encrypted data means that these applications are still a part of the cardholder data environment (CDE) that is subject to PCI compliance and audits. Since token numbers are not able to be tied back to the original PAN, they do not pose such problems, making tokenized data ideal for use in business applications.

Encrypted numbers could work as substitute values for real card numbers in backend business applications.

CARD-BASED VERSUS TRANSACTION-BASED TOKENS

As mentioned earlier, unique tokens can be generated in one of two ways: by the card, or by the transaction.

In the case of a card-based token, there is a life-long relationship between a PAN and a tokenized number. Every time a consumer uses his card at a merchant's store, the same token number is extracted from the vault and provided back to the merchant in the authorization response. (This assumes the payment processor is the creator/keeper of the tokens.)

There is a life-long relationship between a PAN and a tokenized number.

The advantage of a card-based token is that the merchant can tie together a consumer's transactions over time and build a buying history on that consumer. Many merchants want to understand their customers' buying habits, but today it is too risky to assemble a list of transactions that are indexed to a real card number. Card-based tokens enable this process without the risk of exposing sensitive data and without gathering data manually from consumers, such as requesting their phone number or membership sign up.

Taking it a step further, the unique card/token relationship can carry over to other merchants as well, as long as all of the merchants use the same payment processor or facility to generate and store the tokens. This enables the analysis of desensitized data that is shared among affiliated merchants. For example, a national grocer has aligned with a national fuel retailer to allow loyalty points earned at the grocer's stores to be redeemed at the fuel stations. Issuance and redemption of the loyalty points can be based on the consumer using the same payment card at both merchants' establishments.

In the case of transaction-based tokens, a different token number is generated for each use of a card. This type of token is used when a merchant wants to ensure that card data is not being stored in their system between the time in which the payment was authorized and the time in which the merchant receives payment. The drawback is that the merchant loses the ability to associate the token number to a specific customer for the purpose of other business applications. Transaction-based tokens are best suited to small merchants that do not use post-authorization data for any purpose other than settling the day's transactions.

In the case of transaction-based tokens, a different token number is generated for each use of a card. This type of token is used when a merchant wants to ensure that card data is not being stored in their system between the time in which the payment was authorized and the time in which the merchant receives payment.

FORMAT-PRESERVING TOKENS

In its most general sense, a token is just a random series of characters that are not created through any reversible means (such as an algorithm). For the purpose of the payment process, however, the design of the token is important. The token number will fit into most merchant environments without significantly disrupting any business processes if the following design considerations are applied:

- The tokenized number should have the same number of digits as the real card PAN. Observation of this rule is important to ensure that tokenized numbers can easily replace real card numbers in the post-authorization applications, such as business analytics or loyalty marketing, without requiring significant modification of the applications.
- There should be some degree of card number preservation, such as the last four digits of the token being the same as in the PAN. Doing so allows the tokenized number (or a portion of it) to be printed on the customer's receipt, and he can see that there is a reference to his actual credit card number. The customer will not see a difference at the point-of-sale.

ANOTHER USE CASE EXAMPLE FOR TOKENIZED PAYMENT DATA

Let's look at another use case for how tokenized data provides business value beyond just security and PCI compliance.

A grocery store chain has a loyalty rewards program for which customers register by providing basic identifying information such as name, address and phone number. A customer can choose to link a specific payment card or cards to the loyalty program — or not. Some customers feel uncomfortable providing their payment card account numbers on the loyalty program registration form. Moreover, the loyalty rewards are linked to the customer's transactions, and not necessarily to his choice of payment type. Cash transactions receive loyalty rewards, just as electronic payments do.

Like the quick-service restaurant in the previous example, the grocery chain does not store PANs after payment authorization because the data is not needed for chargebacks or returns. The merchant also wants to avoid the hassle of protecting the data to meet PCI requirements and to prevent breaches.

This grocer also has fuel stations where customers can use their loyalty cards at the pump to obtain discounts on fuel. The merchant prefers to have its customers use a payment card at the pump rather than cash, which requires time-consuming interaction with a cashier. As discussed above, the payment card may, or may not, be linked to the loyalty card.

The merchant was having trouble identifying a customer at the fuel pump as a member of the loyalty program if the customer did not have his loyalty card present. The customer had to identify himself to the cashier inside, who would manually apply the loyalty discount to the fuel purchase. This process took time and was prone to mistakes.

Then the merchant implemented data tokenization and tied it to the loyalty program. When a customer uses his loyalty card in-store and pays for his transaction using a payment card, the card's token number is automatically associated with the loyalty card and stored for future reference. When the customer uses his payment card at the pump to purchase fuel, it triggers the loyalty reward discount, whether or not the customer has his loyalty card with him. There's no need for cashier intervention because the loyalty program can be triggered by the payment card alone.

This "automatic association" process allows multiple family members to link their payment cards to one joint loyalty rewards account.

In addition, this "automatic association" process allows multiple family members to link their payment cards to one joint loyalty rewards account. Now, a teenage daughter can fuel up her car at a discount without having to borrow her mother's grocery store loyalty card.

CONCLUSION

Every retailer and restaurant that accepts debit and credit cards as forms of payment is already paying interchange and other fees; it is simply a cost of doing business in a manner that customers prefer. One way that companies can cost-justify those expenses is to get more value out of the electronic payment process. They can do so by getting their own customer data back from the processor in a tokenized format that can be used risk-free in back-end business applications that improve operations or generate new opportunities for the company. The company can share tokens across multiple applications and even with external partners, franchisees or service providers without fear of a data breach because tokens cannot be monetized if exposed or stolen.

One way that companies can cost-justify those expenses is to get more value out of the electronic payment process. They can do so by getting their own customer data back from the processor in a tokenized format that can be used risk-free in back-end business applications that improve operations or generate new opportunities for the company.

RECOMMENDED READING

To learn more how tokenization, in combination with end-to-end encryption, can help merchants secure their cardholder data, reduce their PCI liability, and open new opportunities for business applications, please see:

- First Data white paper: Implementing Tokenization is Simpler Than You Think
- First Data white paper: Data Encryption and Tokenization: An Innovative One-Two Punch to Increase Data Security and Reduce the Challenges of PCI DSS Compliance
- First Data white paper: Where Security Fits in the Payments Processing Chain
- RSA's Speaking of Security Blog: Encryption and Tokenization

First Data™
beyond the transaction℠

Bank of America
Merchant Services

The information contained herein is provided as a courtesy and is for general informational purposes only. This article is not intended to be a complete description of all applicable rules, policies and procedures. The matters referenced are subject to change. Individual circumstances may vary. The information contained herein includes, among other things, a compilation of documents received from third parties. First Data shall not be responsible for any inaccurate or incomplete information. Nothing contained in this presentation is intended to supplement, amend or modify any applicable contract, rule or regulation.

"Bank of America Merrill Lynch" is the marketing name for the global banking and global markets businesses of Bank of America Corporation. Lending, derivatives, and other commercial banking activities are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., member FDIC. Securities, strategic advisory, and other investment banking activities are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, Merrill Lynch, Pierce, Fenner & Smith Incorporated and Merrill Lynch Professional Clearing Corp., all of which are registered broker dealers and members of FINRA and SIPC, and, in other jurisdictions, by locally registered entities. Investment products offered by Investment Banking Affiliates: Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed. ©2011 Bank of America Corporation.