First Data
beyond the transaction

A First Data White Paper

Understanding the Value of Tokens

Introduction

Credit cards are undeniably a vital component of the retail payment environment, and very few merchants can generate any significant revenue without the ability to accept them.

While accepting cards is a crucial requirement for merchants, there are constant and increasing risks to handling credit and debit card data in its native format. For instance, cardholder data is susceptible to theft if it is stored in the merchant environment and used for analytics, loyalty programs, refunds and other back-office processes. Fortunately, using a tokenization solution produces tokens that can be used securely by the merchant as a valuable substitute for card numbers, enabling them to take advantage of the process optimization opportunities provided by this payment method.

Tokenization enables merchants to pursue business tactics that would not practical from a risk management perspective if undertaken using actual credit card data—and with lower security risk, the salient characteristics of the underlying data can be exposed while protecting the merchant and the cardholder. Decomposing the payment mechanism into multiple pieces that are each individually worthless and re-assembling the pieces in a secure environment provides more comprehensive security while imbuing the process with added value.

If the value of tokens to merchants is the ability to safely convert them to revenue without the risks normally associated with credit cards, the value to their customers lies in the increased security of their card data as well as a simpler and more streamlined loyalty program relationship. This paper explains the benefit of tokens and how they can be used productively throughout a merchant's systems and processes.

Why Credit Cards Are Risky

Credit cards can be risky to merchants because they are easily monetized by thieves, and the merchants bear much of the risk of loss if the data is stolen, lost or exposed. In order to establish industry guidelines for handling credit cards, the Payment Card Industry (PCI) Council's Data Security Standard (DSS) explicitly lists the requirements for protecting sensitive cardholder data.

In accordance with industry mandates, multiple authentication mechanisms have been developed to better ensure data security and to prevent fraud. The goal of a layered security solution (like First Data's TransArmor solution) is to layer the defensive technologies of end-to-end encryption and tokenization together to prevent the theft of cardholder data in both transmission and storage.

The costs associated with a cardholder data breach are substantial—and frequently can be the end of the line for a small merchant, which may not be able to absorb tens or hundreds of thousands of dollars in investigation fees and penalties that can result from an incident. According to a report by Symantec Corp and the Ponemon Institute, the average organizational cost of a data breach increased to $7.2 million and cost companies an average of $214 per compromised record in 2010. Both of these numbers are up in comparison to 2009, when the average organizational cost of a data breach was $6.75 million and the average cost per compromised record was $204. Regulators are working to crack down on non-compliant organizations, and are encouraging them to implement required data security controls.

How Tokens Reduce Security Risk

Tokenization reduces security risk by removing sensitive credit card data and replacing it with the tokens. When the first transaction with a particular credit card is performed through a merchant using a tokenization solution, the credit card number is sent to a tokenization vault. This vault then generates a unique token and maps it to the card number. Once this is done, the merchant does not need to present the credit card number again, and can use the unique card-based token instead for all business processes that would have been accomplished with the credit card. All subsequent transactions with that credit card will produce the exact same token, allowing merchants to track individual consumer spending behavior.

Well-designed tokens include a multitude of security features, and typically preserve the format of the original Personal Account Number (PAN) in order to minimize modifications to existing business systems and processes. In the case of First Data's TransArmor solution, the index table that relates the token value to the PAN exists only inside of the processor environment at First Data—there is no way that the TransArmor tokens can be reverse-engineered or algorithmically decoded to produce the PAN. This is achieved by using strong random-number generation processes to produce the first 12 digits and then combining that with the last four digits of the original PAN. The token then resembles the format of a card number without any of the financial value or risk.

Even if the tokens are stolen from the merchant's environment, the thieves are going to be frustrated when they learn that the tokens are worthless outside of that environment. Each merchant has unique identifiers that are factored into the creation and storage of the tokens for their merchant environment, thus preventing token laundering.

Some merchants may have the misconception that as long as the tokens are stored outside of their card data environment, their liability is shifted to the entity storing those tokens, but this is not necessarily true. Merchants will almost certainly be exposed to a proportional amount of liability in the event of a breach, depending on who houses the tokenization vault and what level of indemnification is provided. Merchants should be sure to select a service provider that is clearly qualified and willing to accept the security risks of protecting cardholder data, and for whom security is already a core competency of their everyday business.

Some processors and providers also offer a warranty on the tokens based on the security architected into the system. However, not all service providers are capable of providing this level of safeguards, so merchants are advised to approach all tokenization solutions with caution, and ensure that proper due diligence is performed when selecting a tokenization provider. A model deploying tokenization at the processor versus tokenization in a gateway or third party results in potentially different levels of risk.

By requiring an extra step to monetize the data (i.e., conversion of the token to the PAN at time of settlement), the merchant employs a secure payment mechanism and transfers the risk of holding cardholder data upstream to its processor—the entity best designed to handle that data.

Tokens and PCI Compliance

PCI compliance is an ongoing cost of doing business for merchants. It tends to increase, rather than decrease, on an annual basis. For large merchants, the cost of compliance can be daunting: according to Ponemon Institute's PCI DSS Trends 2010: QSA Insights Report, the average annual cost of Tier 1 merchant PCI compliance is $225,000. Smaller merchants are not subject to quite the same level of compliance costs, but their expenses are not insubstantial.

Tokenization is designed to provide merchants with a way to monetize their transactions by storing and using the resulting data, without the recognized compliance burden of maintaining PANs. Most PCI audits use automated scanning mechanisms to locate 16 digits numbers in merchant environments, with specific qualifiers such as requiring the numbers to pass a MOD-10 or Luhn check. Well-designed tokens are explicitly engineered not to pass MOD-10 or Luhn checks in order to avoid "colliding" with the same number ranges that valid PANs use, and also to prevent false positives when credit card data scans are performed on the merchant's environment. Furthermore, since tokens are not considered PCI data, the three-year PCI data storage restriction does not apply, and the tokens can be stored and used indefinitely.

Tokens as the Lynchpin of a Loyalty Program

Loyalty programs are designed to enhance the merchant's marketing, helping them to sell more products or additional services, sell more often, and sell faster. Given that customers need a unique loyalty program identifier (since their customer names, addresses, etc. are not always unique), why not use a token based on their payment cards? Many merchants have historically used credit card PANs as an index to track customers, but as we have seen above, that business practice results in a high level of security and compliance risk to the merchant.

With tokenization, merchants will continue to own the relationship with the customer, since customer-identifying information exists only at the merchant or the issuing institution, not the processor. For merchants, creating a profile for every customer in some type of registration process is the first step. Next, customers need to register their payment instruments against the profiles. Merchants can provide incentives so that customers attach every transaction to a profile--even cash purchases.

One example of an innovative TransArmor tokenization implementation as the centerpiece of a customer loyalty program comes from the QSR vertical, where a prominent brand operator uses the token to pull all of the data elements together for its new kiosk deployment. The customers come into the store and swipe either their loyalty card or a credit/debit card into a secure swipe reader on an iPad, which results in a token being retrieved from the First Data SafeProxy™ tokenization vault. Using the card-based token, the merchant references its customer database and determines the valid payment instruments that can be used to complete the transaction. Customers also have the option to order via the website or mobile devices, which utilize the same token and integrate both e-commerce and brick-and-mortar data to provide a consistently excellent customer experience.

There are many retailers that seek to offer innovative solutions for mobile offers, customer loyalty programs, daily deals and more—but they all need a way to effectively track customer activity, and tokens are the ideal point of reference to assemble the customer experience.

A New Paradigm for Handling Data

Organizations that implement tokenization will only need the last four digits of the account to identify the transactions in their environments. Nearly all point-of-sale manufacturers now support truncation or masking on receipts, so customers are already accustomed to seeing only the last four digits of their cards on sales receipts.

Just as multifactor authentication requires multiple items to validate an identity, multifactor investigation provides a mechanism to use multiple data elements to validate a transaction—without the associated risk that a merchant is exposed to from trying to match a transaction against a PAN. For example, to locate a disputed transaction within a POS, a batch settlement merchant can use the batch number to go to the relevant batch, and then search those transactions for the matching last four digits for the date, time, and amount of the transaction. In the event of multiple matches—for instance, if the consumer used the same card to purchase the same item for the same price (e.g., multiple $25 gift cards)—then the authorization code can be used to uniquely identify the transaction. In theory, the token could even be printed as a barcode on a receipt, thus allowing the merchant to scan the customer's receipt for returned goods and other record lookups, increasing the accuracy and speed whilst simultaneously enhancing the customer service experience.

Tokens are returned as part of the authorization process, so for a merchant using a batch settlement process, tokens are used as the settlement reference. For merchants using a host capture settlement, the settlement happens via the host, but the tokens may still be returned for storage and use in the merchant data warehouse if so desired, or as part of reconciliation file for increased accuracy, speed and facilitating programmatic matching.

There are some operational differences in how terminal-based merchants do business compared to merchants that rely on point-of-sale (POS) registers, and the best tokenization providers support those differing business requirements. For terminal merchants, if a customer makes a return during the same batch period (before settlement occurs), the merchant simply enters the transaction number into the terminal and processes the return—business as usual. If a customer needs to make a return after the batch period, the merchant uses the customer card or the receipt to process the return, like they have always done.

For POS merchants, if a customer makes a return during the same batch period, the merchant simply scans the receipt, and the POS looks up and voids the transaction within the current batch—business as usual. If the customer presents the card, the POS will send a message to retrieve the token associated with the card, and then match the returned token to the transaction history stored in the POS transaction logs, POS database, or transaction data warehouse depending on the merchant's chosen implementation. If a customer needs to make a return after the batch period, the merchant simply scans the receipt and the POS looks up and voids the transaction within the current batch, as before. And if the customer presents the card, the POS will send a message to retrieve the token associated with the card and then match the returned token to the transaction history stored in the POS transaction logs, POS database, or transaction data warehouse depending on the merchant's chosen implementation.

Conclusion

Using tokenization technology helps merchants decouple the value of customer intelligence from the previously unavoidable risk of handling cardholder data and accepting the associated compliance costs.

If actual PAN data is stored or transmitted inside the merchant environment—even encrypted or truncated—the merchant's environment is in scope from a PCI compliance perspective. By storing and using tokens instead, merchants can reduce their PCI compliance obligations dramatically. Furthermore, long-term storage of encrypted PANs is currently limited to three years, but tokens remove that restriction and allow a merchant indefinite retention, for long-term data trending with all of the additional benefits described above.

Why manage a higher level of risk, liability and cost than necessary? With nearly 300,000 merchants in production and over a quarter of a billion transactions securely processed to date, First Data's TransArmor solution is becoming the de facto industry standard solution for end-to-end encryption and tokenization. Contact your sales representative or visit firstdata.com to learn more.

The Global Leader in Electronic Commerce

Around the world every day, First Data makes payment transactions secure, fast and easy for merchants, financial institutions and their customers. We leverage our unparalleled product portfolio and expertise to deliver processing solutions that drive customer revenue and profitability. Whether the payment is by debit or credit, gift card, check or mobile phone, online or at the point of sale, First Data helps you maximize value for your business.

For more information, contact your First Data Representative or visit firstdata.com

2731