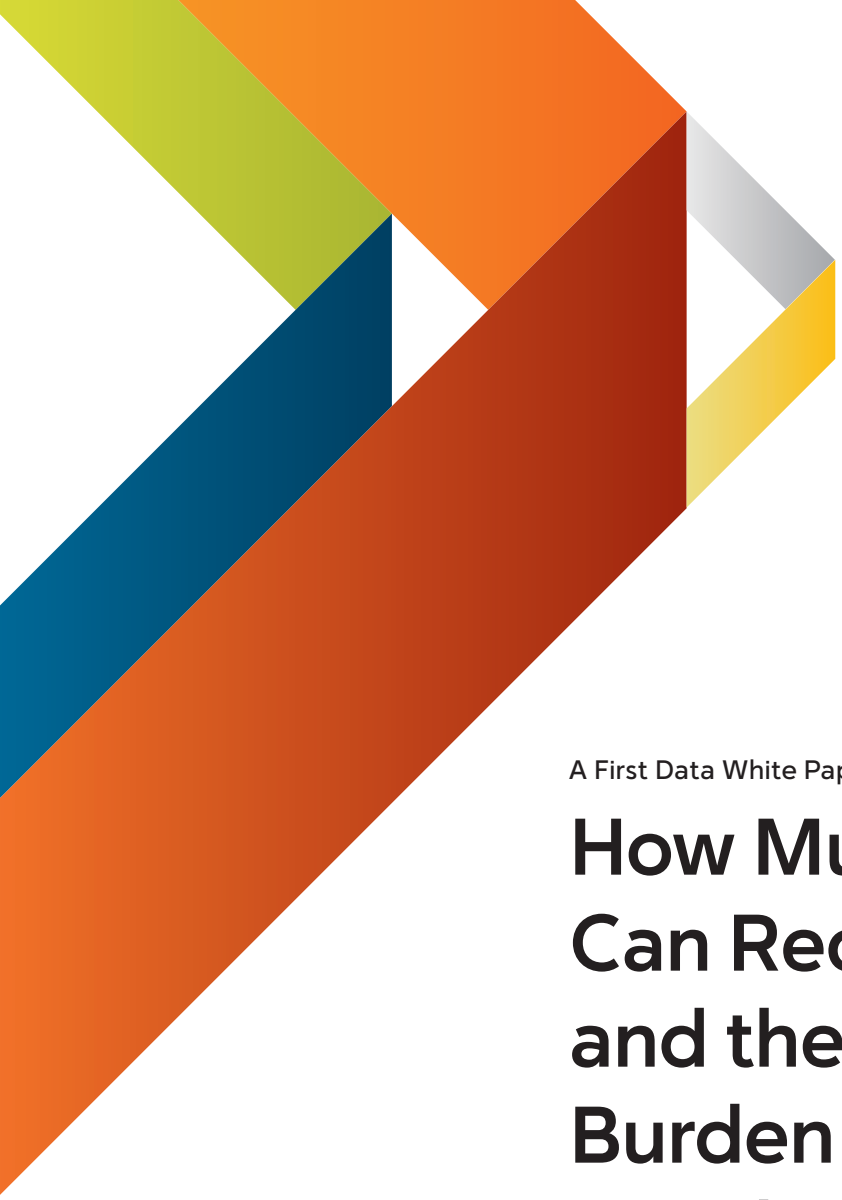


First Data
b›yond the transaction

A First Data White Paper

How Multi-Pay Tokens Can Reduce Security Risks and the PCI Compliance Burden for eCommerce Merchants

Introduction

In spite of a sluggish economy, eCommerce continues to flourish as sales shift from in-store to online. The U.S. Department of Commerce reports that retail eCommerce sales during 2011 increased by 16 percent over 2010, and should continue to experience double-digit growth over the next few years.[i] A recent forecast by Javelin Strategy & Research estimates that the total transaction volume for online retail purchases will reach $429 billion by 2015 in the U.S. market alone.[ii]

As their customer base grows and repeat sales soar, many eCommerce merchants are finding managing data security and meeting PCI compliance requirements to be a significant and growing concern. Every merchant that accepts credit and debit cards is required to be compliant with the Payment Card Industry (PCI) Data Security Standards (DSS), which are intended to reduce payment card fraud by improving the security of cardholder data. The time and cost burdens of PCI compliance in terms of both security implementation and compliance validation depend on the extent to which a merchant collects, stores, transmits or processes payment card data.

Many merchants may be familiar with tokenization, which replaces sensitive data—like a cardholder's primary account number (PAN)—with a "token" that retains many of the required properties of the original data but removes the elements that carry risk. Merchants have embraced the usage of tokens in place of real cardholder data for business processes conducted after a payment transaction is complete. Tokens allow safer long-term storage of transaction data that can be used to support back office operations and analyze customer behavior. What's more, tokens reduce risk and PCI compliance obligations because the merchant is not storing or using account information that can be monetized if stolen.[iii]

A new type of token called a multi-pay token expands the usefulness of tokenization in financial transactions. Multi-pay tokens address the primary security risk and PCI burden inherent in a card-not-present (CNP) environment—the need to store customers' preferred payment information for repeat transactions—making them an ideal solution for eCommerce merchants and service providers with recurring invoices. A multi-pay token can greatly reduce or even eliminate the merchant's liability for both ongoing PAN storage and the initial interaction with the customer's card number (in certain scenarios). In some cases, a merchant can drastically reduce its PCI compliance burden because it *never touches the customer's PAN at all* during a payment transaction.

We'll explore this solution in detail below, as well as use cases for multi-pay tokens in both CNP and card-present situations, and merchant benefits like getting a broader view of the customer experiences and purchasing activity across all sales channels.

What is a multi-pay token?

Tokenization is the process of replacing sensitive data with surrogate numbers that remove risk but preserve value to the business. To tokenize a payment transaction, the PAN is sent to a centralized and highly secure server called a "vault" where it is stored securely in a PCI-compliant environment. Immediately after authorization from the card issuer, a random, unique token number is generated and returned to the merchant's systems for use in place of the PAN. A secure cross-reference table is established to allow authorized look-up of the original PAN, using the token as the index. Without authorization to access the vault and look up the PAN, the token value is meaningless: it's just a random number. If the token is stolen or otherwise accessed by an unauthorized user, it alone cannot be used to perform a monetary transaction.

The original concept of the token meant that the merchant could not use this random number to perform a subsequent financial transaction, because it is not a valid PAN. However, a multi-pay token adds the ability to perform an authorized financial transaction under strict control measures within the merchant environment. The merchant submits a token that it already has on file for a specific consumer/card to a processor with access to the vault to retrieve the PAN and complete the transaction. By using this type of token in the payment authorization process, the merchant reduces the risk of having the real PAN stolen as it is being collected from the consumer or stored by the merchant.

Multi-pay tokens are especially valuable in eCommerce and other CNP environments that tend to store payment card information in a virtual wallet or on their website for repeat customers. The multi-pay token allows a merchant to tokenize the payment card information, associate that token with the consumer profile stored on the merchant side, and then use the token with the processor gateway that holds the token vault in order to run subsequent transactions. This is done without the need to prompt the customer for his card account number again, and without having to store the actual card number.

The merchant's initial transaction with the consumer's payment card uses the real account data, but for all subsequent transactions (e.g., to process refunds, credits and future purchases) that use the same payment card, the merchant can use the token instead. A multi-pay token is unique to a specific card used with a specific merchant. This ensures that one and only one authorized merchant can ever use the token to process subsequent transactions.

Moreover, multi-pay tokens are not limited to eCommerce or even CNP situations. As we'll explain later, they can be used in "brick and click" scenarios for merchants that have physical locations as well as an online presence.

How a multi-pay token is used in an eCommerce environment

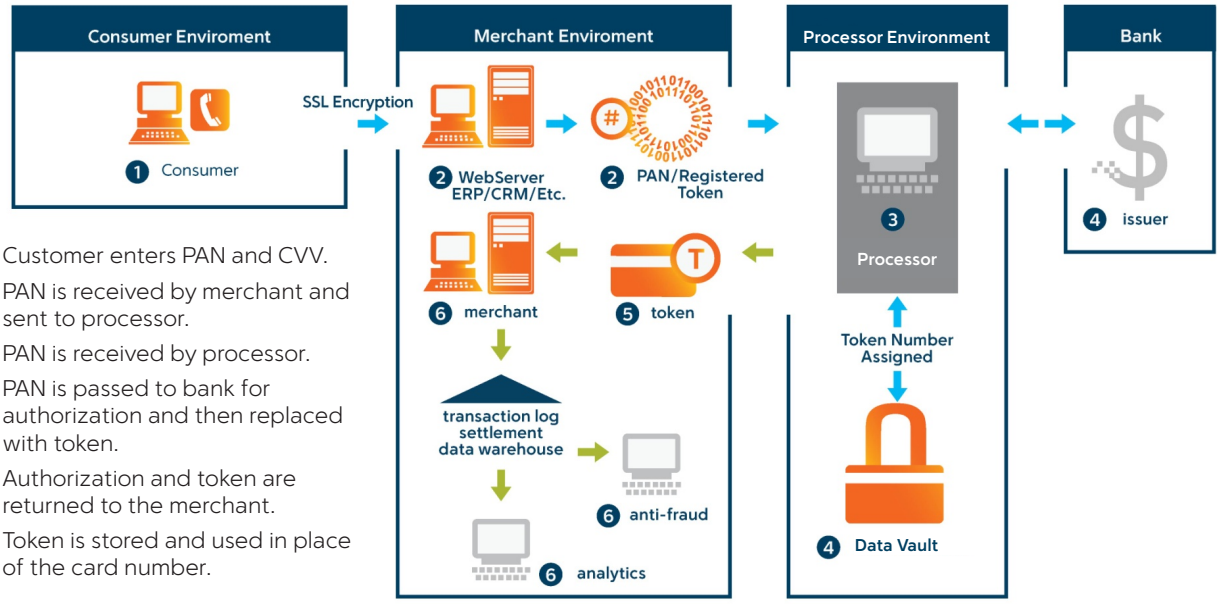
It is common for eCommerce merchants to ask their customers to register by providing profile information such as name, address, and phone number to the merchant website before or upon checkout. The profile may also store or contain a link to the customer's payment card information. Merchants seeking to encourage repeat business offer to store the customer's payment card information as a matter of convenience to reduce checkout time on subsequent visits.

In a traditional environment without multi-pay tokens, the merchant assumes the responsibility of securely storing each customer's payment information for use in subsequent transactions. This creates a security risk as well as a PCI compliance obligation. The merchant needs to provide thorough security measures around the sensitive cardholder data, and must demonstrate that those measures meet the requirements of the PCI regulations. If the data is stolen or otherwise compromised, the merchant may be subject to expensive fines and other penalties.

Using multi-pay tokens reduces or completely eliminates those risks, depending on how the merchant chooses to implement the tokenization process. Let's have a look at how this works.

The first time a consumer makes a purchase on the merchant's website, the checkout process prompts him to provide his payment information, including the credit card account number and card verification value (CVV). The merchant submits this and the other required transaction information to the processor for authorization. The processor returns a multi-pay token to the merchant, who stores it along with the customer's other profile information. When the customer returns to make a subsequent purchase, the merchant can ask, "Would you like to use your credit card ending in 1234?" If the customer says yes, the merchant retrieves the customer's stored multi-pay token from the profile [or linked] database and submits it as the payment instrument in this transaction. Using the secured index database, the processor matches the multi-pay token to the actual PAN in the vault and continues to process the transaction using the real PAN.

TOKENIZATION AND CNP



1. Customer enters PAN and CVV.
2. PAN is received by merchant and sent to processor.
3. PAN is received by processor.
4. PAN is passed to bank for authorization and then replaced with token.
5. Authorization and token are returned to the merchant.
6. Token is stored and used in place of the card number.

This scenario can be executed in two different ways, and how it is done determines how much liability the merchant has for PCI compliance and security risks.

In the first option, the merchant operates its own checkout process, and would typically connect to a processor through an API or other direct connection. The merchant collects sensitive card account information from consumers and maintains liability for that information until it is submitted to the processor to complete the transaction. Once the processor returns a token to the merchant, the merchant does not need to keep the actual cardholder data anymore. Thus, the front end portion of the checkout process is still in scope for PCI compliance and data must be appropriately secured through encryption and potentially other measures.

In the second option, the merchant directs its customers to a hosted checkout gateway page for the collection and processing of the sensitive information. The hosted page can be framed on the merchant's website so it has the same appearance as the merchant's site and provides a consistent customer experience. Technically, however, the hosted checkout is not part of the merchant's environment and thus is not in scope for the merchant's PCI compliance requirements. In this scenario, the merchant avoids touching sensitive payment information at all, and thus has minimal requirements for PCI compliance. Transactions are processed and multi-pay tokens can be returned to the merchant for storage with the consumer profile and use in subsequent transactions and business intelligence.

Merchant Advantages of Multi-Pay Tokens

There are several potential advantages to using multi-pay tokens, including improved security, reduced PCI scope, enhanced analytic capabilities, and a simplified customer profile management process.

Improved security of online data

When non-sensitive tokens are used for payment transactions, there is less risk of criminals stealing data they can monetize. In recent years, there have been very serious data breaches in the eCommerce world in which cyber thieves have stolen customer records containing payment card numbers and bank account numbers. These breaches caused tremendous harm to the merchants involved, as well as to the consumers whose data was stolen.

Multi-pay tokens eliminate that worry. If they are ever intercepted, hacked or exposed, the tokens are useless to anyone but the authorized merchant. Multi-pay tokens have sufficient layered security measures built in so that they can only be monetized by the merchant under very explicit security conditions.

Reduced PCI scope/liability protection

Maintaining and validating PCI compliance is an expensive and time-consuming effort for most merchants. But it's important to remember that "in compliance" is really a state at a point in time, and it is possible to be "PCI compliant" without being completely secure. Multi-pay tokens address both risks of security and non-compliance.

A merchant can vastly reduce or even eliminate the cardholder data environment (CDE) that is in scope for PCI audits by substituting multi-pay tokens for real cardholder data. And by minimizing or eliminating the presence of cardholder data itself, the merchant avoids the cost of protecting that data—reducing its security risk and PCI liability.

Data Analytics

Many merchants find it beneficial to use historical transaction data tied to specific customers in their business intelligence applications. If real card data is used for this purpose, PCI requires potentially expensive and cumbersome security measures, such as encryption, to protect the data. By using non-sensitive tokenized data, the merchant can freely use the transaction information for various purposes, including data analysis and customized marketing programs to help refine the business and drive additional customer visits and sales.

Customer Profile Management/Recurring Payments

As mentioned earlier, most eCommerce merchants ask customers to register by providing basic profile data, as well as payment card information, if desired. By storing multi-pay tokens instead of live cardholder data, the merchant vastly simplifies its customer profile management processes in a way that is seamless and imperceptible to customers. Customers' preferred payment information can be stored and used repeatedly without jeopardizing sensitive data. Payment gateways may also offer merchants the ability to pass customer I.D. numbers, e-mail addresses, and other indicative information along with the transactions. This data, as well as the multi-pay token, helps provide an accurate view of the merchant-consumer interaction.

Taking this concept a step further, the customer profile data can be linked to a merchant's loyalty program. Each time a multi-pay token is used for a purchase, the token can trigger the loyalty program to allow the customer to accumulate or redeem rewards at the time of purchase.

Five Example Use Cases: Putting Multi-Pay Tokens to Work

In the sections below, we describe how multi-pay tokens can be used in both online and offline environments where the payment card is not present. They also can be used in "brick and click" scenarios where a merchant has both physical and virtual locations. The tokens can be linked to stored customer profiles, and an innovative merchant can use multi-pay tokens in association with a customer loyalty program.

1. Standard eCommerce Scenario

In this scenario, the merchant hosts its own checkout application and customer profile database. When a new customer registers to use the website, he provides personal profile information such as name, address, website username and password. Either at this time or upon first checkout, the customer is prompted to enter his card account data for one or more preferred payment cards.

When the merchant submits the initial payment transaction from this customer, the processor returns a multi-pay token which is forever associated with that customer using that card with this specific merchant. (Note that this initial transaction can be a zero dollar amount that is strictly for the purpose of generating the multi-pay token.) The merchant stores the multi-pay token and links it to the customer profile; the real cardholder data never has to be stored by the merchant.

The next time the customer logs into the website to make a purchase, he selects his preferred payment card from those that he previously entered. The merchant retrieves the customer's appropriate multi-pay token from storage and uses it to complete the transaction securely and efficiently.

2. eCommerce Scenario with Hosted Payment Page

This next scenario is very similar to the one above, except now the merchant has elected to use a hosted checkout service rather than hosting its own. A customer still registers on the website and provides personal profile information (but not payment information). However, when he goes to checkout, the merchant website transparently transfers him to a hosted payment service.

When the customer makes an initial purchase, the hosted payment service collects the customer's payment card information, generates the multi-pay token and sends it to the merchant, which then permanently associates it with that customer. The hosted service stores the merchant's multi-pay tokens for future use (this data can also be transferred to the merchant to use for analytics). When a customer makes a purchase from that merchant's website, the hosted payment service retrieves the stored multi-pay token associated with that customer, payment card and merchant. (Note that multi-pay tokens are unique to each merchant that subscribes to the hosted payment service.)

3. Multi Channel Scenario

A multi-pay token is a card-based token, which means the same token is employed each time a specific card is used. (Compare this to a transaction-based token, where a new token is generated for each transaction—even those initiated by the same customer.) A multi-pay token is unique to a specific merchant, which ensures that no other merchant can use the token to complete a transaction.

These qualities of the multi-pay token allow a token to be used throughout a merchant's retail channels, including physical store locations, an eCommerce website, and mail/phone/fax orders. Future channels can be accommodated as well; for example, shopping applications on smart devices. This provides the ultimate flexibility for the innovative merchant that wants to drive sales through customer convenience and choice.

As described in the previous scenarios, a multi-pay token is generated the first time a customer has a card-based transaction with the merchant—even if that transaction takes place in a physical store. For all subsequent CNP purchases made through the merchant's sales channels, the multi-pay token can be used to complete the transaction. On the back end, the merchant can use the multi-pay token as an index to aggregate the customer's entire transaction history, regardless of the sales channel.

4. Service Provider with Recurring Invoice Scenario

Not every CNP transaction is an eCommerce purchase. There are many types of service providers that need to collect a regular payment from a consumer over a sustained period by processing a credit or debit payment. Examples of merchants in this category include newspaper and magazine publishers, utility companies, property rental agencies, insurance agents, and even healthcare providers that offer billing plans. Smaller organizations in this segment are ideal candidates for the hosted payment gateway service described above.

Once again, for a customer's first payment, real card data is submitted to the processor and a multi-pay token is returned for the merchant to use. With authorization from the customer, the merchant simply submits the token to the processor on a regular basis (such as monthly) for a payment transaction.

5. Loyalty Program Scenario

Many merchants today have a customer loyalty program designed to increase sales through repeat purchases and larger tickets. By necessity, a merchant's loyalty program collects and stores customer profile data, which could include a customer's preferred payment information. Any merchant that collects and stores such payment information must ensure its security and be prepared to verify the security processes in a PCI compliance audit—or, the merchant can store multi-pay tokens instead.

When a customer swipes either his loyalty card or a registered payment card, the processor can retrieve the token associated with that card and use the token to complete the loyalty transaction. The merchant can apply or redeem loyalty rewards for that customer as appropriate.

Conclusion

Multi-pay tokens represent a significant advancement in conducting secure CNP transactions for recurring payments or repeat customers. Because this unique type of token can be used to complete most financial transactions, the merchant enjoys all the functionality of a PAN, with a high level of protection against the theft or exposure of sensitive payment card data—without investing heavily in layered data security solutions. In addition, multi-pay tokens reduce or eliminate the merchant's cardholder data environment, which in turn reduces the scope, time and cost of PCI compliance requirements and audits.

The optimum level of security enabled by the use of multi-pay tokens occurs when a merchant employs a hosted payment application. In this case, the merchant never has to collect or touch cardholder data at all. Moreover, the merchant can still use the resulting multi-pay tokens for subsequent transactions and in back office applications to analyze historical transaction information.

Merchants can use multi-pay tokens in various ways—with or without a card being presented—to offer enhanced convenience to customers, which in turn can help the merchant deepen the customer relationship and capture a larger share of the growing eCommerce market.

For more information about multi-pay tokens, contact your account representative or visit www.FirstData.com.

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.

Sources

[i] U.S. Dept. of Commerce website; eMarketer blog post, Healthy Growth for Ecommerce as Retail Continues Shift to Web, March 17, 2011.

[ii] *The Green Sheet*, "Going Global with Online Payments," January 9, 2012.

[iii] Securosis, "Understanding and Selecting A Tokenization Solution," 2010.