Carat

Reducing PCI Scope With Omnichannel Tokens

Carat

Introduction

Twenty years ago, the idea of buying something online was almost inconceivable; today it's not just ubiquitous, it's quickly taking its place as the major competitor to the way we've shopped for generations: by physically visiting a store.

As one study notes, "COVID-19 has caused us to vault five years forward in consumer and business digital adoption in a matter of around eight weeks. Consumer behaviors and preferred interactions have changed significantly and the uptick in the use of digital services is here to stay. Seventy-five percent of people using digital channels for the first time indicate that they will continue to use them when things return to "normal."

Of course, stay-at-home orders due to the COVID-19 outbreak have only increased the number of customers opting to shop online in card-not-present (CNP) situations. "Third quarter 2020, eCommerce sales increased 37 percent from the third quarter of 2019 while total retail sales increased 6.9 percent in the same period. eCommerce sales in the third quarter of 2020 accounted for 13 percent of total sales" per the U.S. Census Bureau of the Department of Commerce (DOC)".

As online shopping has grown in popularity, so too has the ease of paying for goods and services electronically. Growing in popularity are voice-activated devices such as Amazon's Alexa and Google Home, which allow consumers to order and pay for goods simply by verbally requesting them. Products can also be ordered using smart watches; and consumers are able to purchase goods directly from the screens of their connected vehicles.

Consumers are not just paying online; they're registering with their favorite stores, providing online retailers with personal information in addition to their preferred ways to pay.

As their customers grow and repeat sales soar, many eCommerce merchants are finding that managing data security and meeting PCI compliance requirements are significant and growing burdens.

Every merchant who accepts credit and debit cards is required to be compliant with the Payment Card Industry (PCI) Data Security Standards (DSS), which aim to reduce payment card fraud by improving the security of cardholder data.

Carat Fact

Managing data security and meeting PCI compliance requirements are significant and growing burdens.

The best way to protect payment data at rest is through the use of tokenization. This technology replaces sensitive data, such as a cardholder's primary account number (PAN) with a token, an unrelated number that nevertheless retains many of the required properties of the original data. Tokens enable safer long-term storage of card data.

To more easily protect that data, "multi-pay" tokens give merchants the ability to utilize the token for subsequent card-on-file transactions. This makes multi-pay tokens an ideal solution for eCommerce merchants and service providers submitting recurring invoices.

Carat

In this White Paper, we'll explore the concept of multi-pay tokenization, its varied use cases in CNP and card-present (CP) situations and the multiple ways in which multi-pay tokens benefit merchants in terms of security, compliance, liability, reduced costs, customer satisfaction and the ultimate ability to increase sales.

You may already be working with Carat, a leading provider of data protection technologies or you may be simply wishing to learn more. In either case, in the following pages you'll learn how you can maximize your protection and grow your business, by allowing Carat to do what we do best: serving your interests and needs.

Carat

Reducing PCI Scope With Multi-Pay Tokens

Tokenization is the process of replacing sensitive data with unrelated surrogate numbers; tokens are randomly generated and a PAN cannot be derived from the associated token.

Multi-pay tokenization provides the ability to initiate financial transactions using the token in place of the PAN. The merchant submits a token that it has on file for a specific consumer's credit card, to a processor that has vault access; the PAN is retrieved by the processor and the transaction completed.

Multi-pay tokens have increased in importance due to the rapid growth of eCommerce transactions. Today, it's the norm rather than the exception for consumers to return to their favorite websites, mobile apps or IoT devices again and again to make purchases. Having established an online account, consumers do not want to have to reenter payment information each time a transaction is made. At the same time, consumers expect that their data will be protected once stored on a business' eCommerce site.

Carat Fact

Due to the shift to digital payments multi-pay tokens are growing in importance

An important feature of multi-pay tokens is that they are unique not only to the particular PAN but also to that merchant; only the merchant can use the token to process subsequent transactions, making it highly resistant to theft. While the merchant's initial transaction with the consumer's payment card uses the real account data, all subsequent transactions (for example: to process refunds, credits and future purchases) with the same payment card use the token instead.

Multi-pay tokens are not limited to eCommerce or even CNP situations. As we'll explain later, they can be used by merchants that have a physical location and online presence, a so-called "brick and click" model.

Carat

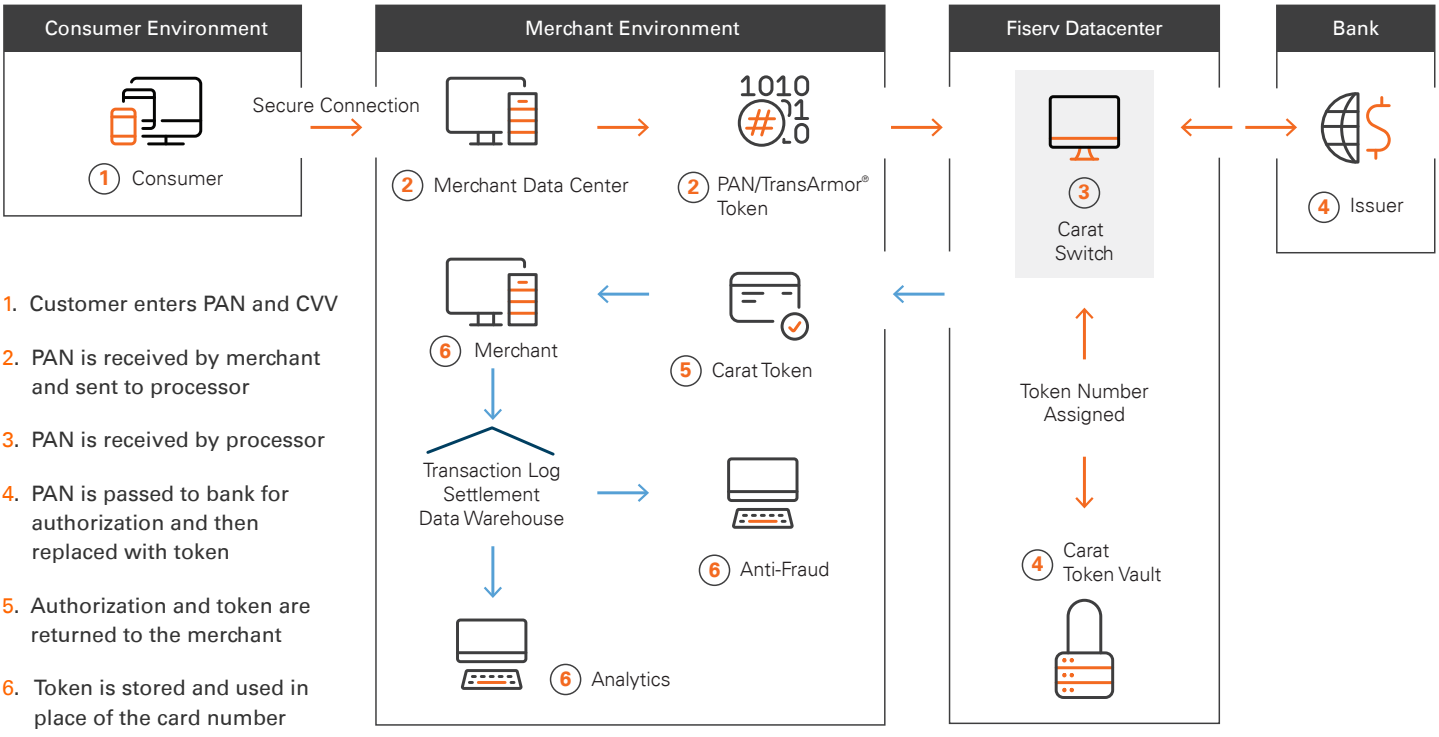
How a Multi-pay Token Is Used In Omnichannel Environments

Merchants seeking to grow repeat business encourage customers to store their payment card and profile information as a matter of convenience, in order to reduce checkout time on subsequent visits.

When multi-pay tokens are not used, the merchant assumes the responsibility for securely storing each customer's payment information for use in subsequent transactions. If the data is stolen or otherwise compromised, the merchant may be subject to expensive fines and other penalties.

Merchants who employ multi-pay tokens reduce those security risks and obligations. Under an eCommerce scenario, the first time a consumer makes a purchase on the merchant's website, the checkout process prompts the customer to provide his or her payment information, including the credit card account number. The merchant submits this and the other required transaction information, through a secure connection, 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.

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

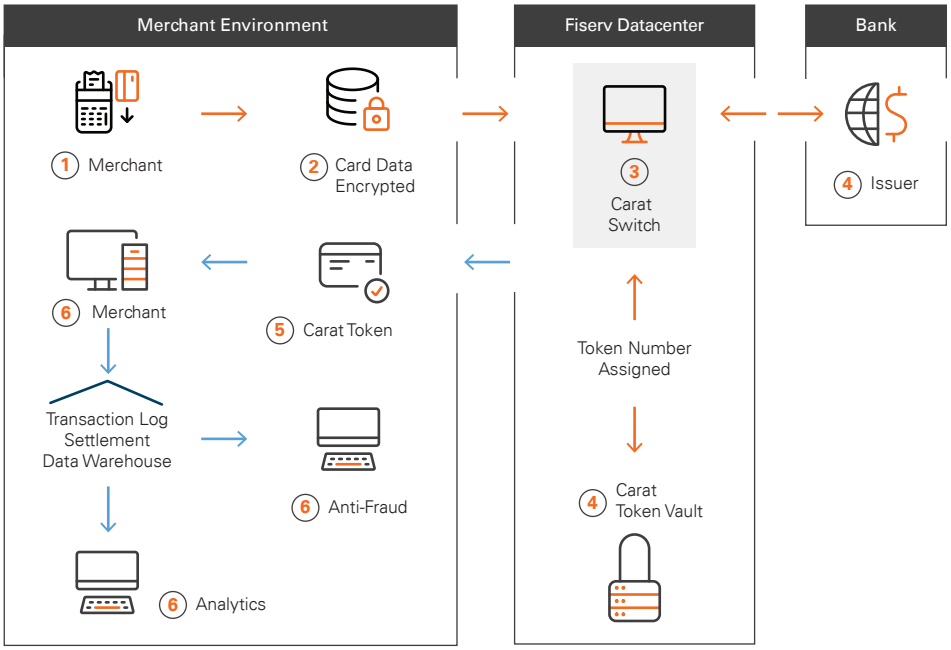
Carat

Carat Fact

Using a token instead of PAN data in back-end business applications shrinks the merchant's cardholder data environment that is subject to PCI compliance.

Omnichannel merchants utilize a similar transaction flow for Card Present payments initiated across devices. As before, the payment information is gathered during checkout and sent to the processor. The Processor returns a consistent multi-pay token which works across the merchant's environment.

Tokenization and CP



1. Consumer presents card to merchant
2. Card Data is encrypted and transmitted to Carat front-end
3. Carat front-end decrypts the data payload
4. Card data is sent to issuing bank for authorization and in parallel, tokenized
5. Token is paired with authorization response and sent back to the merchant
6. Merchant stores token instead of card data in their environment and uses token for all subsequent business processes

Carat

Merchant Advantages of Multi-pay Tokens

There are several potential advantages to using multi-pay tokens; they include improved merchant security, reduced PCI scope, enhanced analytic capabilities and a simplified customer profile management process. In addition to their use in digital transactions, multi-pay tokens can also be used in omnichannel, "brick-and-click" situations.

Improved Security of Online Data

When non-sensitive tokens are used for payment transactions, there is less risk of criminals stealing data they could otherwise monetize.

For the merchant, a breach can incur a hefty fine, as well as legal and remediation costs. Breaches of up to 10 million records cost an average of $50 million, taking into account fines, detection costs, notification costs, reputation loss and litigation. (Source: Ponemon Cost of a Breach 2020 report)

Costs can substantially exceed that average amount. For example, in August 2020, the Office of the Comptroller of the Currency fined a major provider of credit cards an $80 million civil penalty for failing to adequately protect its consumer database from a successful hack of 100 million files by a disgruntled former employee of Amazon Cloud Services.

Carat Fact

In 2020, a major credit card provider was fined **$80 million** for exposing the data of **100 million** files.

Other companies that have been fined include a major foreign air carrier, which had to pay $230 million to its government and a large hotel chain, at a cost of $124 million.

Consumers who abandon the merchant due to a breach can cause long-term damage to sales; those customers could also take legal action against the merchant due to identity loss and the costs of repairing their credit history.

Multi-pay tokens eliminate the worry of data theft. If they are ever intercepted, hacked or exposed, the tokens cannot be used outside of the merchant's environment.

Reduced PCI Scope/Liability Protection

Maintaining and validating PCI compliance is an expensive and time-consuming effort for most merchants. Furthermore, being "in compliance" is a dynamic state that may only be true at a particular point in time; and one may be PCI compliant without being completely secure. Multi-pay tokens address risks of security and non-compliance.

Omnichannel tokenization allows merchant to replace sensitive card data with Tokens. Multi-pay tokens are returned in place of the PAN for CP and CNP transactions. Merchants can store the multi-pay token and vastly reduce or even eliminate the required cardholder data environment (CDE) that is subject to PCI audits, while also avoiding the cost of protecting that data.

Omnichannel Capabilities

Multi-pay tokenization provides omnichannel capability, allowing one token to be used throughout a merchant's diverse retail channels. Given the wide variety of use cases, multi-pay tokenization becomes an excellent tool to help drive sales, as it maximizes customer convenience and choice.

Data Analytics

Many merchants find it beneficial to use customer-specific transaction data in their business intelligence applications. By using non-sensitive tokenized data, the merchant can safely use the transaction information for data analysis and customized marketing programs. This can help increase business efficiencies and aid in the creation of strategies designed to increase customer visits and sales.

Customer Profile Management

By storing multi-pay tokens instead of cardholder data, merchants vastly simplify their 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. The multi-pay token helps provide an accurate view of the merchant-consumer interaction.

Customer profile data can also 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, enabling the customer to accumulate or redeem rewards at the time of purchase.

Recurring or Subscription Payments

Carat Fact

Multi-pay tokens can be used to securely ID your consumer across your entire payment footprint (CP and CNP)

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 include streaming services, subscription services and utility company payments. Multi-pay tokens allow merchants to store a token in place of the PAN and use for future transactions, as long as that PAN is current.

Conclusion

As has been shown, multi-pay tokens are the ideal way to simplify the payment process in an environment in which eCommerce is taking an increasingly dominant role. Multi-pay Tokens protect PCI data allowing a merchant to safety store payment data for future transactions.

Merchants can use multi-pay tokens across their environment offering enhanced convenience to customers. This helps deepen the customer relationship and the ability to capture a larger share of the established and growing eCommerce market.

Multi-pay Tokens represent a significant advance in conducting secure transactions for Card Present, eCommerce, digital, recurring or subscription payments. Because this unique type of token can be used to complete a financial transaction, the merchant enjoys all the functionality of a PAN, plus a high level of protection against the theft or exposure of sensitive payment card data, all without investing heavily in layered data security solutions.

And when it comes to choosing a multi-pay token provider, note that Carat applies best-in-practice tokenization security to protect customer card data. Carat tokens are not reversible, do not expire and follow the customer's card through its life cycle.

Carat multi-pay tokens are available either directly or from one of our over 75 certified gateways and software vendors. Using a direct connection or a certified vendor guarantees that data is tokenized during the transaction flow from the merchant to Carat, ensuring that card data is never sent in the clear.

Unlike standard Data Protection, gateway tokenization solutions only tokenize data between themselves and the merchants. Gateways must detokenize their token and send it to processors in the clear, thereby exposing card data at the last mile between the gateway and the processor. In this less-desirable scenario, the merchant would be responsible for the entire transaction flow from a PCI perspective: from their site to the processor's.

Carat tokens provide a consistent security solution across the entire payment environment, obviating the need to use multiple, complex security solutions from various payment applications for customer and payment management.

In summary, Carat enables a business to focus on growth and customer service, utilizing tokenization technologies to easily and cost-effectively implement data security best practices.

Carat Multi-pay Token Features and Benefits

Features:

- Unlike encryption, a token has no direct relationship with the data that it replaces
- The token is card-based, meaning there is a 1:1 relationship between the PAN and the token
- Multi-pay tokens do not expire – The same token follows the card through the entire card lifecycle
- The token matches the length of the initiating PAN and maintains the last 4-digits
- The token does not overlap BIN ranges from major card brands, including those of Amex, Discover, Mastercard and Visa
- Tokens do not pass the Luhn or MOD-10, algorithm

Carat is the omnichannel commerce ecosystem that delivers unlimited global payment opportunities across any channel anywhere, executing transactions on any device with any payment method, securely and at global scale.

Omnichannel tokenization offers improved security of online data and can help reduce PCI scope, which offers liability protection to merchants. This value is currently offered by Carat and can be accessed through the Commerce Hub.

Through simple API access, Carat enables merchants, experience providers and financial institutions to imagine and realize new customer experiences.

Carat drives more commerce.

For more information, contact your account representative or visit merchants.fiserv.com/carat.

Sources:

[1] mckinsey.com/business-functions/mckinsey-digital/our-insights/the-covid-19-recovery-will-be-digital-a-plan-for-the-first-90-days

[2] census.gov/retail/mrts/www/data/pdf/ec_current.pdf

[3] Ponemon Cost of a Breach 2020 report

[4] theverge.com/2020/8/8/21359761/capital-one-80-million-fine-2019-data-breach

© 2021 Fiserv, Inc. or its affiliates. All rights reserved. Fiserv is a registered trademark of Fiserv, Inc. Other products referenced in this material may be trademarks or registered trademarks of their respective companies. Terms and Conditions apply.