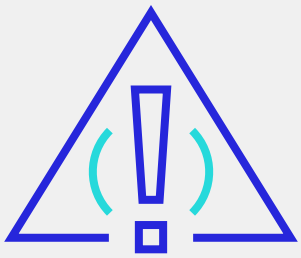
Navigating the Challenges and Benefits of Tokenization

ACI Worldwide
Real-Time Payments



Executive Summary

Tokenization of data has undeniable advantages for retailers, yet it can raise some important challenges for fraud prevention strategies.

High-profile data breaches have been making regular headlines in the last few years, with millions of customer records being compromised each year. The impact of data breaches can be far reaching. Not only is there a very immediate and direct cost associated with the loss itself, but falling victim to a breach can also cause business interruption and damage the customer experience — leaving a lasting effect on brand reputation, customer loyalty and profitability.

While any kind of organization can be the victim of a data breach, stealing identity information and payment card data is the easiest way for hackers to monetize their activities and convert their crimes to cash — making merchants among the most profitable targets for hackers. Merchants are also open to internal theft if payment card information is stored without strong protection measures designed to prevent their own employees from using the payment card details illegally.

1 The Value of Tokenization for Retailers

Understandably, tokenization solutions are gaining popularity as a response to these issues, with a 2016 study by the Ponemon Institute[1] indicating that 72% of respondents understand that the ability to encrypt or tokenize sensitive or confidential data is important, and 86% say it will become more important over the next two years. A survey by ACI Worldwide and Forrester Research in 2015 indicated that only 34% of retailers were using tokenization technology at that time, with a further 36% conducting pilot programs.

Tokenization, which replaces the primary account number (PAN) with a unique value or numeric sequence, renders transaction data useless to thieves because they are unable to reverse the process to uncover the original data. This is why tokenization can play a crucial role in the payments security continuum, helping to protect sensitive information, prevent the damage caused by data breaches and deter hackers.

The growing use of "card-on-file" models among merchants is continuing to accelerate token usage and, as a result, many of the key players in mobile payments and eWallets are now using tokenization as a key part of their payments security strategy. They are able to use the approach to store unique tokens in a customer's eWallet, which the customer can then use to make purchases — all

1 The 2016 Global Cloud Data Security Study, Ponemon Institute

without the merchant needing to receive the card details or PAN. This approach can serve to enhance the security of digital payments and simplify the customer buying experience when shopping on mobile or other smart devices.

Deploying a tokenization solution can also help to improve security in cross-channel transactions which combine card-present and card-not-present elements. For instance, the second part of a cross-channel transaction (for example, where a customer reserves goods online and collects them in store) can use a token to complete the transaction, relying on the payments system to fill in the original card details.

Tokenization solutions that work across multiple channels, also referred to as omni-token solutions, lay the foundations for these and other new customer journeys, provided merchants work with a vendor who is able to support them in all their channels.

Added to all this, using a token system can help to minimize or even eliminate the need for merchants to store payment card data, so reducing the scope of PCI DSS compliance. By eliminating the storage of sensitive data in back-end systems (post authorization) and replacing it with tokens, these systems do not have to be assessed for PCI DSS.

By formatting tokens in the same way as card information, the impact to merchants' back-office systems can be minimized. Tokenization solutions are also global and compatible with existing payment technologies and networks, while supporting future payment technologies.

2 Practical Challenges and Considerations

Despite its undeniable advantages, tokenizing payments data can cause some complex challenges for retailers, in particular with regard to implementation and fraud prevention.

Implementation Challenges

Since chargebacks typically take 30-60 days to process, merchants must consider how best to handle card details during implementation to ensure that chargebacks can be reconciled with the card details held on file. One option would be for retailers to run tokens alongside the card numbers for a set period in order to create a smoother transition process.

Order reconciliation can create similar issues when it comes to returns and issuing credits, so it is important for merchants to ensure the same transaction ID is used from authorization to settlement.

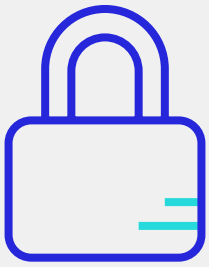
Velocity rules specific to card numbers will also be impacted during the transition period and merchants need to understand the potential implications of fraud going undetected. Testing the token and its format is imperative to velocity rules, to ensure low false positives while still detecting unique tokens.

Fraud Prevention Implications

It is important for any existing negative or positive customer lists (black and white lists) specific to card numbers to be tokenized to ensure continuity of customer experience and maintain fraud prevention levels.

Applying single-use tokens (where a new value or token is generated every time a card is used) can seriously hinder a retailer's ability to perform link analysis and use velocity rules. Multi-use tokens (using a fixed token for each card across every transaction) can allow a retailer to continue using these vital fraud detection strategies to full effect.

It is imperative, as part of an optimized fraud rule set, to understand and analyze a number of factors around each transaction in order to conduct effective real- time screening. This makes it important for retailers to retain the bank identification number (BIN) which defines the issuer, card type and country of issuance — all crucial data points for fraud detection and pattern identification.



Often consumers may not have their receipt or know their transaction ID when looking to return goods, causing reconciliation challenges if the card information has been tokenized. Retaining the last four digits of a card within a token can help to create a smooth customer experience and also help with the authentication and verification process.

Lastly, if merchants are signed up to a fraud intelligence service which provides cross-merchant fraud data, it is possible there may be some devaluation of the external fraud intelligence, since each merchant will send a different token for the same card when it is used across retailers. Ideally, either the fraud solution provider needs to receive the original payment card information or, better still, there needs to be some relationship between the fraud management service and the tokenization service.

3 Summary

Tokenization can deliver very tangible benefits in securing payments information: preventing the loss of sensitive data and protecting businesses against reputational damage.

However, even as the use of tokens grows, it will not be enough on its own to prevent fraud. Any channel can be leveraged by fraudsters — regardless of whether the payments they make go through a tokenization process or not.

It is vital that merchants continue to equip themselves to detect and prevent any and all fraudulent activity in addition to protecting the payments data itself. Tokenization must, therefore, be considered as one part of an effective, integrated payments security and fraud prevention strategy.

As with any part of this payments security continuum, it is critical that tokenization solutions are properly configured to take into account the potential impact across systems and operations which interact with the customer, to ensure that the right balance is achieved between loss mitigation and a good customer experience.

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com
@ACI_Worldwide
contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ATL1344 07-21

ACI Worldwide
Real-Time Payments