First Data
beyond the transaction

First Data Market Insight

Avoiding a Data Breach: An Introduction to Encryption and Tokenization

In 2012, 621 confirmed data breaches were reported in the United States, resulting in the theft of over 44 million sensitive consumer records—including millions of debit and credit card account numbers.[1] Data breaches are constantly in the news, and recent high profile cases show that no organization is immune—especially as criminals develop increasingly sophisticated methods to exploit vulnerabilities in the payment system.

All merchants have both an obligation and an industry mandate to protect consumers' payment card data. The Payment Card Industry (PCI) Data Security Standards (DSS) provide guidelines on what merchants need to do to secure the sensitive data used in payment transactions. End-to-end encryption (E2EE) and tokenization solve for many of the vulnerabilities that exist in the payments processing chain. When combined, these two technologies provide an effective method for securing sensitive data wherever it exists throughout its lifecycle.

Vulnerabilities in the Payment Process

Card data for a purchase transaction must flow through multiple systems and parties in order to be processed. For most merchants, there are two points in the payment process where sensitive cardholder data is at risk of being exposed or stolen:

1. Pre-authorization – When the merchant has captured a consumer's data and it is being sent or is waiting to be sent to the acquirer/processor.
2. Post-authorization – When cardholder data has been sent back to the merchant with the authorization response from the acquirer/processor, and it is placed into some form of storage in the merchant environment and used for analytics and other back-office processes.

Fortunately, there are highly effective technologies available to address these two specific points of vulnerability: encryption and tokenization. Encryption mitigates security weaknesses that exist when cardholder data has been captured but not yet authorized. Tokenization addresses security vulnerabilities after a transaction has been authorized.

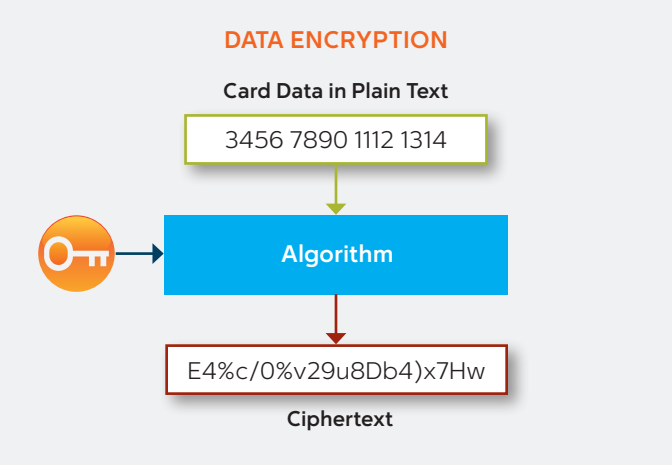
[1] Verizon RISK Team, 2013 Data Breach Investigation Report, April 2013.

Encryption

Encryption is the process of using algorithmic schemes to transform plain text information into a non-readable form called ciphertext. A key is required to decrypt the information and return it to its original plain text format.

Any time that live cardholder data is in the clear—that is, in plain text format that is readable by a person or computer—it is extremely vulnerable to theft. Of course, criminals know this and look for ways to capture that data. For example, it's possible for a thief to siphon off the card data as it is transmitted in plain text from a card reader to the point of sale (POS) server or the merchant's central server. Encryption of either the data itself or the transmission path the data takes along the network, or both, can vastly reduce the vulnerability of the data, which in turn reduces a merchant's security risks.

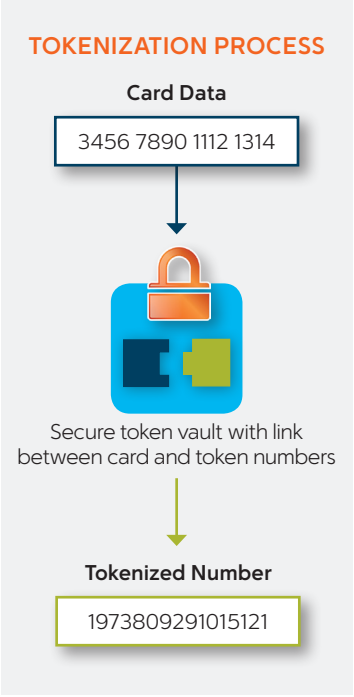
There are multiple approaches to encryption in the payment process, including session-level encryption versus data-level encryption, symmetric versus asymmetric encryption, and software-based encryption versus hardware-based encryption (see First Data's white paper, What Data Thieves Don't Want You to Know: The Facts About Encryption and Tokenization for more information on these technologies). A merchant will need to evaluate its own environment to determine which approach or approaches would work best to meet its needs.



Avoiding a Data Breach: An Introduction to Encryption and Tokenization

Tokenization

A proven method for protecting sensitive data post-authorization is the use of a token as a replacement for a real payment card number. In the process of tokenization, once the transaction is authorized the payment data is sent to a centralized and highly secure server where it is stored. At the same time, a random unique number is generated and returned to the merchant's systems for use in place of the cardholder data. The token number—which cannot be monetized by anyone but the merchant that owns the token—can be used in subsequent post-authorization business processes.



Tokenization is important for two reasons. First, it vastly reduces a merchant's security risk in the event of a data breach because it eliminates sensitive cardholder data from a merchant's environment after a transaction has been authorized. If token numbers are breached, they are meaningless to data thieves because they are simply random numbers. Second, using token numbers instead of real card data in back-end business applications shrinks the merchant's cardholder data environment (CDE) that is subject to PCI compliance requirements and audits. This reduction of PCI scope can save a merchant significant time and money. The PCI Security Standards Council notes: "Tokenization solutions do not eliminate the need to maintain and validate PCI DSS compliance, but they may simplify a merchant's validation efforts by reducing the number of system components for which PCI DSS requirements apply."[2]

As with encryption, there are multiple approaches to tokenization (e.g., card-based tokens or transaction-based tokens). Which approach is best for a merchant depends on how the merchant plans to use the tokenized numbers in its business applications.

Protecting Your Data

Payment security is complex, with risks and vulnerabilities at every point of the processing chain. The combination of increasingly burdensome PCI compliance costs and constantly emerging new data security threats make it essential for merchants to implement effective risk management technologies to limit costs and avoid the disastrous consequences of a data compromise event.

Encryption and tokenization solve for mutually-exclusive security weaknesses in the payments process, and in doing so, can reduce a merchant's PCI scope and compliance costs. Encryption protects data that has been captured by the merchant but has not yet been used for the transaction authorization process. Tokenization solves the problem of storing and using real card data in business processes that are downstream from authorization.

Although neither encryption nor tokenization is currently required by PCI DSS, the combination of these technologies is widely recognized as the most powerful way to protect against data theft. The First Data TransArmor® solution makes cardholder data significantly more secure by combining encryption and tokenization for superior protection. For more information about implementing a comprehensive data security solution to protect vulnerable card data, please contact your sales representative or visit firstdata.com.

The First Data TransArmor® solution makes cardholder data significantly more secure by combining encryption and tokenization for superior protection. It is an easy-to-implement payment security service that removes card data completely from the merchant environment, protecting customer's sensitive information, limiting merchant liability and simplifying PCI compliance.

The First Data TransArmor Solution

1. Completely removes payment information from the merchant environment
2. Reduces PCI compliance scope, effort and cost
3. Shields merchant from liability for breaches
4. Offers multiple encryption options
5. Is cost-effective and easy to implement
6. Preserves a unique card-based ID (Multi-pay tokens) to support recurring payments in a No Card Present environment

Beyond the transaction℠

[2] PCI Security Standards Council, Information Supplement: PCI DSS Tokenization Guidelines, August 2011

6203