OMNIFUND
Payments as a Platform®

Tokenization and Transaction Security for the Omni-Channel Environment

Disclaimer

This White Paper was prepared by OmniFund and reflects OmniFund's interpretation of relevant credit card association rules and regulations. This White Paper is for general informational purposes only, and OmniFund recommends that the reader consult directly with the appropriate credit card association with specific questions regarding the interpretation of any Visa or MasterCard rule or regulation.

Executive Summary

Over the past few years, as the avenues to receive and send payments electronically has increased into an Omni-Channel environment, PCI compliance requirements have evolved in such a manner as to create a burden on most companies struggling with a desire to secure client data while also remaining in compliance with ever changing rules and IT landscapes. Many companies, inexperienced with transactional security related issues, are finding the cost of conformity prohibitive and burdensome. Changes to public facing and backend systems must be checked against current PCI regulations resulting in additional time to market, and IT expenses related to product and service modifications and PCI documentation. Additionally, the storage of client transaction data necessitates a third-party review of facilities, processes, and code, adding yet another layer to compliance. Tokenization and transaction security are one part of the effort to combat these issues with an additional focus being on how to remove an organization as far from PCI scope as possible.

Effectively, compliance is good only in the moment attained, but it does not mean that a business is still compliant after that. In ever-changing business environments, there is always an opportunity for compliant status to change. A company might not be aware that a password or process is modified inadvertently or a software application has been newly discovered to have a security vulnerability, exposing them to a data breach. Equally as important, companies should be aware of the danger of relying on generalists (be they sales people or processor representatives) as a reliable source of guidance. These individuals, while well meaning, have an agenda to "close a deal," and are ill equipped to handle complex compliance and IT issues.

It is critical that the PCI-DSS process is regarded as an ongoing initiative. Common areas of vulnerabilities include:

- Outdated Point of Sale (POS) systems
- Storing payment card data, or missing critical updates
- Remote access granted to your POS vendor
- Default passwords on software not changed
- Lack of firewalls, proper network security, or anti-virus software
- Paper-based records physically accessible, not guarded or locked

Whether initiated through manually captured, electronically captured, or automated transfer of payment card data, each step of the transaction flow should be assessed with regards to how payment card data may be exposed. The more a third-party provider can do to provide their clients with step-by-step guides or best practices documentation, the more effective the engagement process.

Simply acknowledging PCI issues is not enough. Rarely can a business with specialization outside of data security meet or exceed PCI requirements on their own. The requirements are too complex and dynamic resulting in huge expenses in time and money to develop effective information security processes. Additionally, the economy of scale acts to work against a business attempting to "go it alone" who try to recreate systems that are easily incorporated using a reliable third party provider like OmniFund.

Omni-Channel Environments

Businesses today are finding that clients are demanding more ways to pay for goods and services than ever before. A mix of payment methods including face-to-face, online, mobile, electronic invoicing, and customer portals, are becoming an increasing part of the payment landscape for most businesses. Omni-Channel payment networks used by clients include not only credit cards but ACH, eCheck, Check 21, Apple Pay, Google Wallet, and PayPal, just to name a few. To remain competitive, and at the same time facilitate faster payment compliance, businesses will need to embrace numerous payment channels. There must be a be willing to either keep up with the regulatory and technological developments over time or partner with an expert, third-party companies adept at providing services that remove this burden from businesses while providing Omni-Channel payment options to consumers.

Part of a risk analysis involves identifying all items both physical and virtual that need protecting. Some things are obvious like the various pieces of hardware or cardholder data. Others are apt to be overlooked, such as people who have access to the systems. It is essential to identify all things that could be affected by a security problem or potential threat and determine how best to ensure compliance of each. A list of categories should include:

- Data. Stored online, archived off-line, backups, audit logs, databases, in transit over a communication medium, during execution, and during delivery (physical or otherwise). Included is cardholder data, merchant specific data, ACH files, contract information, rate information, contact information, etc.

- Supplies. Paper, forms ribbons, magnetic media.

- Hardware. Including CPUs, keyboards, terminals, terminal servers, routers, firewalls, disk drives, communication lines, printers, personal computers, laptops. It should include not only the hardware used for actual processing but also the hardware used to view data and access the data. It might also include hardware systems used for access to the facilities and systems (tokens or smart cards).

- Software. Often includes source programs, utilities, backup operating systems, communication programs, object programs, the source code itself, web content, e-mail and network systems.

- People. Users of the systems, people needed to run operations, contract personnel for hardware and software. The U.S. Department of Commerce lists insiders as the number one threat to information.

- Documentation. Documentation often is overlooked. Proper documentation should include programs, hardware, systems, local and remote administrative procedures.

Tokenization

Tokenization is a method used to protect data and covered within PCI-DSS guidelines as a preferred method to handle sensitive consumer data. PCI-DSS guidelines and compliance usually meet or exceed federal, state and consumer guidelines and regulations as related to the privacy and handling of customer data. While tokenization will not remove a business from PCI scope, it may significantly reduce audit and notification requirements as well as possibly reducing documentation compliance related workflows.

While several methods of tokenization are viable, the best method is a tokenization strategy in which tokens are stored with external service providers or networks inside Certified Level 1 PCI-DSS systems. Tokens created and stored on local systems provide very little in the way of additional security and certainly increase the workload and sophistication required to accomplish in scope tokenized transactions.

At OmniFund, tokenization is done entirely in-house through our proprietary process, and no third-party service is utilized to provided tokenization of sensitive data. OmniFund tokenization provides a secure way to collect sensitive consumer data and convert it into a non-identifiable token. These tokens can then be stored and used in subsequent transaction requests and to ensure that sensitive account holder data is never stored on, or communicated to, systems external to the PCI Level 1 server environment. Additionally, tokens may be stored along with non-identifiable account data (account-holder name, expiration date, etc.) to allow an easy way to identify and manage the individual accounts while still allowing integrations to operate under current PCI guidelines.

OmniFund employs customized tokenization to randomly generate an alpha numerical string which in and of itself does not have any relation to the original data. For example:

- Id card number 4111111111111 is entered – the token request will respond with a token formatted like "tok_33j339d4494fj94k493op". Token "tok_33j339d4494fj94k493op" is then used to process all future transactions. If a business necessity dictates the need to view card information, then the last four digits of the card and expiration date associated with the token can be displayed within a local system. While this permits the business to be PCI compliant, the scope of compliance and documentation requirements may increase.

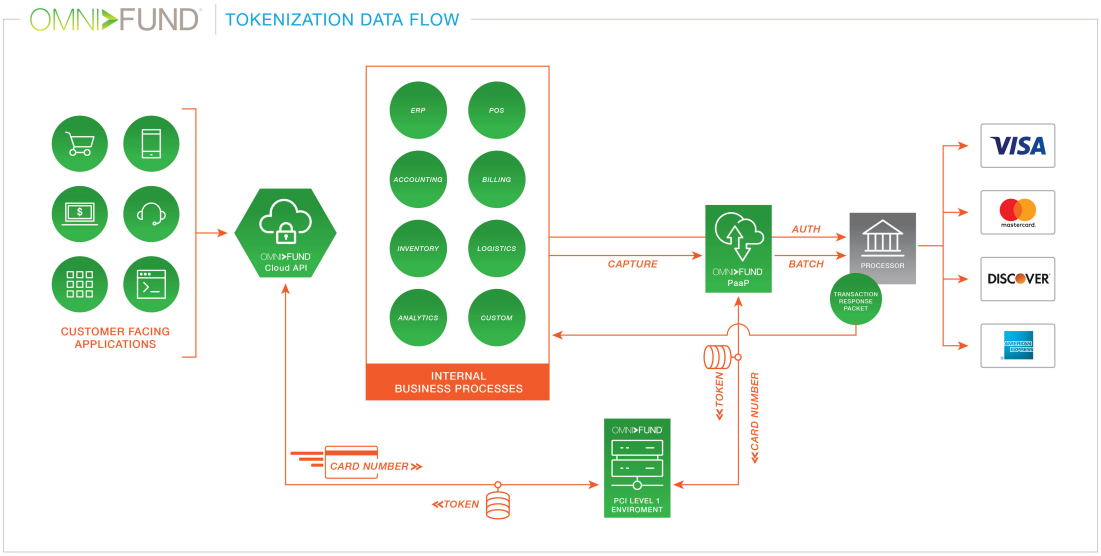
Third-Party Provider Advantages

The temptation by some businesses to manage PCI issues internally may seem like a less expensive or easier path to compliance. However, unless the company has dedicated IT staff thoroughly trained on security compliance and is willing to remain permanently engaged with the ever-changing PCI and regulatory environments, internal compliance efforts will cost the business much more regarding monetary value and opportunity cost. This is due to having internal resources focus on activities outside of the business' core revenue generating activities. Third-party providers offer the fastest, least expensive and most efficient method to ensure that a company remains as far out of PCI scope as possible. The burden to keep up with regulatory rules and technological changes fall squarely on the shoulders of the third-party provider.

Tokenization provided by a third-party vendor competent in PCI matters can significantly reduce your risk of a data breach. If it is unnecessary to store a credit card number for settlement or recurring charges the business' exposure is isolated to the initial authorization transaction. While significant exposure remains, tokenization eliminates the exposure that stored information represents.

It is important to note that the use of localized tokens provides no reduction in a business' obligation to comply with PCI DSS. It is a fact that the adverse effects of performance degradation may far outweigh any benefits of tokenization.

Third-party providers focused primarily on security, and secondarily on payment processing, are the best source and authority for businesses looking to develop long-term reliable and dedicated compliance support. These firms employ staff PCI specialists to assist with compliance issues, technology updates, and code enhancements to the primary systems handling sensitive data. In addition to being a Certified PCI-DSS Level 1 Service Provider, OmniFund has a certified PCI-DSS ISA with CISSP Certification (internal security auditor) on staff to provide laser focus on regulatory changes and system updates, processes and change management. Additionally, OmniFund is a QIR Certified Integrator and Reseller adding to the expertise within the staff at OmniFund.



Beyond Tokenization – Moving 100% Out of Scope

While tokenization provides a method of securing sensitive data it remains only a limited way relative to removing a business payment process from PCI scope. Tokenization still requires many steps on the part of the business to ensure internal processes are compliant, even though tokenization methods are employed. A company that uses tokenization remains in PCI scope and must still deal with all the cumbersome requirements of monitoring internal personnel (eyes on data), paper data handling, network security, and route threat scanning.

OmniFund is employing patent pending methodology designed to ensure that no human or system inside a business or business process has access to, or indeed ever encounters, consumer payment data. These methods utilize the latest available technology and are designed to provide users with transaction security confidence, while at the same time removing participating business out of PCI scope entirely.

To find out more about how OmniFund can help you move your financial systems and processes 100% out of scope, please visit www.omnifund.com or contact us at sales@omnifund.com today.

Reference Material

PCI-DSS Security Standards Counsel - https://www.pcisecuritystandards.org/

Visa USA - https://usa.visa.com/content/dam/VCOM/download/merchants/Visa-Data-Security-Program-Keeping-Cardholder-Data-Safe-VOL-02.06.13.pdf

MasterCard - https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations.html

What Merchants Need To Know About Security - https://www.mastercard.us/en-us/merchants/safety-security/security-recommendations/merchants-need-to-know.html

Tokenization Guidelines - https://www.pcisecuritystandards.org/documents/Tokenization_Guidelines_Info_Supplement.pdf

Contact Info

OmniFund®
Payments as a Platform®

Steve Eyring
Executive V.P. Business Development
Steve.Eyring@omnifund.com
Direct: (385) 232-5084