

# New Tokenization Guidelines and TransactionVault™

An overview of the guidelines document on tokenization put forth by the PCI Security Standards Council and how Merchant Link's tokenization solution meets these guidelines.



On August 12, 2011, the Payment Card Industry Security Standards Council (PCI SSC) issued an Information Supplement to provide guidance on how to implement a tokenization solution and how it may impact the scope of a merchant's compliance efforts with the PCI Data Security Standard.

Already, there have been a lot of questions and buzz around this in the industry and the first question we want to answer for our customers is "Does Merchant Link meet these new guidelines?" More specifically, "Does TransactionVault meet these guidelines?" The answers are YES – we not only meet these guidelines, we exceed them.

## Guidance Document Excerpts and Merchant Link Solution Detail

### **2.1.1 Whichever [token] generation method is used, the recovery of the original PAN must not be computationally feasible knowing only the token or a number of tokens.**

Merchant Link tokens cannot be "reverse-engineered" back to the original PAN. The actual generation of a token is through a complex multi-step algorithm, but we take care to ensure that the original PAN cannot be derived from the token.

### **2.1.2 The ability to retrieve a PAN in exchange for its associated token should be restricted to specifically authorized individuals, applications, and/or systems.**

We recognize that there are real business needs to exchange a token for its original PAN, but we restrict that action to authorized and authenticated users.

### **2.1.3 Because it contains PANs as well as tokens, the data vault often presents the most attractive target for attackers. Compromise of the data vault could potentially result in the compromise of the entire tokenization system, and additional security controls above and beyond those required in PCI DSS may be warranted.**

We recognize that merchants have put their faith in Merchant Link's ability to keep their card data secure. We are in the security business. It's what we do well, so that merchants can focus on and excel in their core businesses. Additionally, Merchant Link is a PCI Level 1 Service Provider and audited continuously, and as such we have significant controls around access to the data vault.

### **2.2 As a general principle, tokenization and de-tokenization operations should occur only within a clearly defined tokenization system that includes a process for approved applications to submit tokenization and de-tokenization requests.**

Absolutely. When we work with new merchants or technology partners, we generally give a lot of advice as to how their tokenization and de-tokenization systems should work. We want tokenization (and especially de-tokenization) to occur in carefully-designed, controlled environments.

### **2.3.2 Only authenticated users and system components should be allowed access to the tokenization system and tokenization/de-tokenization processes. The authentication method should categorize all endpoints, including but not limited to applications, people, processes, and systems, to ensure the appropriate level of access is granted.**

Merchant Link uses a layered system of access and authentication, from IP filtering to user name and password to security certificates. Automated systems monitor and report on access to sensitive data in real time. Alerts are generated in the Merchant Link 24x7 Network Operations Center (NOC) when unauthorized access to sensitive data is attempted.



### 2.3.3 The tokenization system should provide comprehensive and robust monitoring.

Our TransactionVault tokenization system is monitored 24x7x365 by our experienced Network Operations Center. Any anomalous behavior or transaction is immediately escalated.

### 2.3.4 The tokenization solution should include a mechanism for distinguishing between tokens and actual PANs.

The algorithm we use allows our merchants and us to distinguish between tokens and PANs.

### 2.3.5 Because the tokenization system stores, processes and/or transmits cardholder data, it must be installed, configured, and maintained in a PCI DSS compliant manner.

Merchant Link's PCI-compliant and segmented network infrastructure securely isolates and protects cardholder data. Continuous, real-time security logging, activity monitoring, and alerting proactively ensure that only authorized protocols and network traffic transit our network to and from trusted networks and hosts. Alerts are automatically generated when unauthorized protocols or network traffic are detected. The security status of all network devices and systems is vigorously monitored to ensure that all Merchant Link network infrastructure and systems remain secure and PCI-compliant at all times.

### 4.1 An important consideration when evaluating a tokenization solution is whether the token itself can be used in lieu of cardholder data to perform a transaction... Tokenization solutions which support these types of tokens should have additional controls in place to detect and prevent attempted fraudulent activities.

We agree that there needs to be controls placed on tokenization systems that utilize these "high-value" tokens.

We accomplish that in two ways:

- With robust, multi-layered access and authentication controls.
- By restricting who can use the token. Merchant Link tokens can only be used to perform a transaction at the merchant that was the original recipient of the token.

## PCI DSS Scoping Considerations

Many merchants believe that use of a tokenization system will take them completely out of scope for PCI. As this new guidance document points out, that is not correct. What tokenization does is *minimize* the Cardholder Data Environment (CDE), thus minimizing a merchant's risk of card data being compromised, while also reducing costs for ongoing PCI compliance. Ultimately, determining what is in and out of PCI scope for a merchant depends primarily on the systems and controls in place in the merchant's environment as well as the assessment conducted by a Qualified Security Assessor (QSA).

## Our Commitment to Data Security and Innovative Solutions

We understand how critical the security of your customers' information is to you. Each year, we invest millions in our infrastructure to ensure our systems are current and configured to meet the strictest security and compliance standards and benchmarks. We also require all employees to complete a detailed security awareness training program and repeat this program annually, as content is constantly updated to reflect current security challenges and concerns.

Since our founding in 1993, Merchant Link has focused on removing the risk and hassle of payments for merchants. We remain committed to developing innovative solutions such as TransactionVault to allow you to focus on your core business without worrying about managing and protecting your customers' cardholder data.

## Let Us Answer Your Questions

Whether you have questions about your PCI compliance or our TransactionVault solution, we're here to help. Contact us at [sales@merchantlink.com](mailto:sales@merchantlink.com).