****

**Customer Vault Guide**

PCI Certified Storage of Customer Payment information

Customer Vault Overview 2

Customer Vault Process Flow 2

Value Proposition 3

# Customer Vault Overview

**Security Concerns**

The Customer Vault was designed specifically for businesses of any size to address concerns about handling customer payment information. Visa and MasterCard have instituted the Payment Card Industry (PCI) Data Security Standard to protect cardholder data–wherever it resides–ensuring that members, merchants, and service providers maintain the highest information security standard.

These associations have also deemed that merchants will be held liable for any breach of cardholder data. This has become a major concern for merchants who may handle credit card or electronic check payments, but are looking to avoid the tremendous costs and resources involved in becoming PCI compliant.

**Customer Vault Solution**

The Customer Vault allows merchants to transmit their payment information through a Secure Sockets Layer (SSL) connection for storage in our Level 1 PCI certified data facility. Once the customer record has been securely transmitted to the Customer Vault, the merchant can then initiate transactions remotely without having to access cardholder information directly. This process is accomplished without the merchant storing the customer’s payment information in their local database or payment application.

Furthermore, using the gateway’s 3 Step Redirect Method in conjunction with the Customer Vault allows merchants to process transactions **without transmitting any payment information** through their web application. This unique approach provides best of class application flexibility without any PCI compliancy concerns. The 3 Step Redirect API (Advanced Programmers Interface) is available by request of the project manager.

# Customer Vault Process Flow

**An initial Customer Record creation using the Customer Vault**

1. The Cardholder securely submits sensitive payment details *directly* to the Customer Vault.
2. The Payment Gateway performs the requested operation and the results of the transactions are returned to the Merchant’s web application. Simultaneously, a Customer Vault token of “12345” which contains all customer data including payment details is created.
3. The Merchant’s web application displays the appropriate message to the customer as to whether the transaction was approved or declined.

***30 days later, Merchant wishes to charge the customer again using Customer Vault token “12345”***

1. The Merchant’s web application connects to the Customer Vault and remotely loads customer record “12345” to initiate a $50.00 charge.
2. The Payment Gateway processes the transaction and responds to the merchant with the transaction response from the processor(s).



# Value Proposition

Merchants who utilize the Customer Vault can process transactions and maintain an up-to-date customer database without storing *any* customer payment details. All sensitive customer data was transmitted through encrypted channels and authorizations, captures, refunds and settlements were managed remotely without storing any cardholder data locally. This gives the merchant unparalleled application flexibility while shifting its liability of PCI compliancy.

The Customer Vault can store both credit card and electronic check payment details. Access to the Customer Vault is granted through a secure online interface. The interface specification is described by an API (Advanced Programmers Interface) Integration Manual which is sent by request to the project manager. The Customer Vault and Payment Gateway interface has been Level 1 PCI compliant since 2004.