

Credit Card Security Policy and Compliance for Merchants

Credit card fraud is on the rise. In response to that fact card associations have been making significant efforts to educate merchants on how to handle the cardholder's information securely. It is in the best interest of the State of Alaska to remind employees of the secure nature of credit card holder information. As a merchant the State of Alaska must comply with the Payment Card Industry – Data Security Standards.

Below is a list of security issues and policies, please inform all personnel who work with credit card holder data in your department of these security policies:

- ✓ Merchants are required to transmit your Sales Data to U.S. Bank/Elavon on the same business day that such Sales Data is originated.
- ✓ Merchants will exercise reasonable care to prevent disclosure of Card information, other than to your agents and contractors for the purpose of assisting you in completing a Card transaction.
- ✓ All e-commerce applications that accept credit card payments over the internet will adhere to the Payment Card Industry – Data Security Standards (PCI-DSS).
- ✓ Do not use vendor-supplied defaults for system passwords.
- ✓ When completing a customer transaction, check that the Card is signed. If the Card is not signed, inform the customer that their Card must be signed before a transaction can take place. Have the customer sign the Card in your presence showing a valid government ID that has been signed. If the customer refuses to sign the Card, politely request an alternate method of payment.
- ✓ Do not transmit unprotected PANs (Primary Account Number) by end user technologies (for example, email, instant messaging, or chat).
- ✓ When completing a customer transaction, be aware that the last four digits of the customers PAN and the name on the Card match what is on the receipt. If a discrepancy occurs, discretely alert your supervisor and ask for a “Code 10” authorization. Your supervisor will then call the authorization center for further instructions.
- ✓ Any time a customer does not want a receipt for a transaction; the receipt must be disposed of in a secure manner. See the policy below.
- ✓ Sensitive cardholder data must be disposed of in a secure manner when it is no longer needed for business or legal reasons. You are required by the Associations to store original documentation of each transaction for at least six months from the date of the respective transaction, and to retain copies of all such data for at

least 18 months from the date of the respective transaction. If at all possible, DO NOT STORE CARDHOLDER DATA. If cardholder data must be stored for a short time, store all media containing card numbers in a locked area limited to selected personnel. Prior to discarding any media containing cardholder information, the party will destroy all hardcopy materials by either cross-cut shredding, incineration or pulping so that cardholder data cannot be reconstructed.

- ✓ The full contents of any track from the magnetic stripe are not to be stored under any circumstances. This data is alternatively called full track, track, track 1, track 2, and magnetic-strip data.
- ✓ All point of sale (POS) devices, card terminals, cash registers, etc, must mask out all but the last 4 digits of the card number. If you produce duplicate copies of a sales receipt from a POS device it is acceptable to have the full number on the merchant copy, but the customer copy **must** mask all but last 4 digits. If your POS terminal does not already do this, contact U.S. Bank/Elavon and request an upgrade to the terminal software that will mask the number appropriately.
- ✓ Each user of U.S. Bank/Elavon's reporting tools must have a unique username and password. This password must be changed every 45 days.
- ✓ Any time an employee's responsibility or job duties change such that they no longer need access to card holder data, the user's logon to credit card reporting systems must be deleted immediately.
- ✓ Maintain a policy that addresses information security for your employees and contractors.
- ✓ A log must be maintained to track all media that is moved from a secured area. Management approval must be obtained prior to moving the media.
- ✓ Do not store card numbers in a database.
- ✓ Never store the CVC code. The CVC code is a 3 digit security code printed on the back of the card only.
- ✓ Have reasonable procedures in place to ensure that each card sale is made to a purchaser who actually is the cardholder or the authorized user of the card.
- ✓ The amount of a refund/adjustment cannot exceed the amount shown as the total on the original Sales Data.
- ✓ Managers must update the validation date according to PABP/PA-DSS for any equipment used to process credit card transactions (for example, but not limited to card readers, dial up terminals, or registers).

- ✓ All wireless credit card terminals must be locked in a secure area over night.