



MOTO/Internet Account Guidelines

As a MOTO/Internet account, we strongly suggest the following guidelines when Processing Visa and MasterCard Transactions to prevent any fraudulent or potentially dangerous transactions from affecting your account.

We recommend that you DO NOT SHIP to Africa (Nigeria), Russia, Singapore, or Middle Eastern Countries due to the significant amount of fraud currently encountered in those regions. If you ship to those countries, PRIORITY will suspend the funding, investigate the transaction and potentially hold the funds until the Chargeback window has expired OR the transaction may be disallowed all together! All other overseas shipments will be reviewed by management before being processed.

The following are general guidelines to help prevent chargeback's due to fraudulent manually keyed transactions.

- Authorize all card-not-present transactions- All internet or manually keyed transactions need an authorization. Authorization should occur prior to any service being performed or any merchandise is shipped.
- Request CVV2- The three digit security number is printed on the back of visa cards to help validate the customer is in possession of the card when placing an order. When the customer provides you a CVV2, submit this information along with any additional transaction data (account number and card expiration date) for electronic authorization.
- Verify the billing address with AVS- AVS is an automated fraud prevention mechanism that will allow you to check cardholders billing address as a part of the electronic authorization process. Verifying the address will help give you another indicator of whether or not a transaction is valid.

* For your protection and to avoid having your funding delayed, please consider faxing transaction information to Priority Payment Systems prior to charging your customer's credit card.(866-232-7882) If you are unsure of the legitimacy of an order, this will allow us time to verify with the bank that the cardholder is making the purchase.



PCI Data Security Standard

In addition to taking advantage of the Cvv2 and AVS fraud prevention services, it is strongly suggested that you comply with the (PCI) Data Security Standard. The purpose of the Data Security Standard is to reflect a “wall of security” for your cardholders. By following these guidelines you can assure your customers that their bankcard account number and other personal information is being protected against trespassers.

1. Install and maintain a firewall configuration to protect data
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect shared data
4. Encrypt transmission of cardholder data and sensitive information across public networks
5. Use and regularly update ant-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to data by business need-to-know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to cardholder data
10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security

Should you have any questions concerning a transaction or any other issue please feel free to contact Atlas.

866-395-6625

865-381-1410 (Fax)