

Credit Card Processing, Storage and Security

1) Security

- a. Orders are placed using industry standard 128bit SSL (Secure Socket Layer) encryption to ensure a safe and secure shopping experience (Supported by all major browsers, including Internet Explorer, Opera, Mozilla Firefox and Safari).
- b. Bright Stores utilizes AES (Advanced Encryption Standard) for encryption tasks. More information can be found at:
http://en.wikipedia.org/wiki/Advanced_Encryption_Standard and
<http://csrc.nist.gov/CryptoToolkit/aes/aesfact.html>.

2) Storage and Processing

- a. Credit Cards are handled in one of two ways: database or gateway.
 - i. *Database*
Using the “database” method of credit card handling stores the credit card number in the Bright Stores database. Each credit card/CVV2 number is encrypted using SHA and private keys before being saved. Numbers can be retrieved from the control panel (username and password restricted area), which uses 128bit SSL encryption for maximum security.
 - ii. *Gateway*
Credit Cards entered into a store with the gateway method enabled are not stored on the Bright Stores system and are instead sent to a third party payment processor, such as Authorize.net using 128bit SSL encryption. Only the last four digits of the user’s credit card number are stored within the system.

3) PCI Compliance

From Wikipedia.org (http://en.wikipedia.org/wiki/PCI_DSS): “PCI DSS stands for Payment Card Industry (PCI) Data Security Standard (DSS). It was developed by the major credit card companies as a guideline to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing, storing, or transmitting credit card numbers must be PCI DSS compliant or they risk losing the ability to process credit card payments.”

Bright Stores follows the strict PCI Compliance rules and is monitored on a regular basis by ScanAlert (<https://www.scanalert.com/>).