
# PCI Data Security Standard Compliance

To ensure the protection of our customers, we proactively protect account data and our overall payment systems against the threat of compromises. To assist us with such protection we securely store Visa and MasterCard account data in accordance with the Payment Card Industry (PCI ) Data Security Standard.

***To demonstrate our compliance to our customers we utilize the following tools:***

- On Site Reviews
- Security Self-assessments
- Security Scans

**How Do We Ensure Protection of Account Data?**

To make certain our customers account data is protected we employ the following 9 requirements which comprise the Payment Card Industry Data Security Standard:

1) Maintain multiple firewall configurations to protect data.

2) Do not use vendor-supplied defaults for system passwords and other security parameters.

3) Protect Stored Data.

4) Encrypt transmission of cardholder data and sensitive information across public networks.

5) Use and regularly update anti-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.

Jordan M. Ulch
Chief Operations Officer
Florite International, Inc.