RBS Activewear/Thunder Bridge Trading Company
Credit Card Storage Authorization Form

By signing below, I authorize RBS Activewear/Thunder Bridge Trading Co. to store the credit card information I supplied to them on _____ for my most recent order(s). In addition, by signing this authorization form I acknowledge that if at any time there are invoices that are 30 days overdue on my account my credit card will be automatically charged.

Date: mm/dd/yyyy

_____

Customer Name – *Please Print*

_____ _____

Customer Signature Date

RBS Activewear/Thunder Bridge Trading Co. uses a 3rd party vendor titled PayJunction to store all credit card information in an online vault. This allows us to be PCI level 1 complaint and better protect your information.

How does this work?

- PayJunction uses a form of tokenized data storage, which means all cardholder data is replaced and only the payment processor can decode the card information.
- PayJunction annually has independent auditors test their security systems to ensure PCI compliance.
- Our in-house information system never stores the credit card information, keeping access to credit card information as limited as possible.
- PayJunction regularly updates and implements best practices as they arise so they continue to maintain PCI Level 1 security.

There are 12 top level requirements under the PCI-DSS PayJunction complies with to be Level 1 PCI Compliant:

Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data
- Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder data

- Protect stored cardholder data
- Encrypt transmission of cardholder data across open, public networks (e.g. internet/World Wide Web)

Maintain a vulnerability management program

- Use and regularly update anti-virus software on all systems commonly affected by malware (e.g. PCs and servers)
- Develop and maintain secure systems and applications

Implement strong access control measures

- Restrict access to cardholder data by business need-to-know
- Assign a unique ID to each person with computer access
- Restrict physical access to cardholder data

Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data
- Regularly test security systems and processes

Maintain an information security policy

- Maintain a policy that addresses information security