The Honest Company, Inc. Information Security Policy

Payment Card Industry Data Security Standard

Effective as May 16, 2016

Introduction

The Payment Card Industry Data Security Standard (PCI DSS) provides minimum requirements to maintain the security of cardholder data. PCI DSS applies to all card brands including Visa, MasterCard, Discover, JCB and American Express. Organizations that process, store or transmit credit card are subject to this standard. PCI DSS requirements change as there are new threats to payment card information and this policy will be updated periodically to reflect that.

The Honest Company collects credit card payments in a number of channels including eCommerce, Wholesale and Retail. There are required policies, processes, and technologies applicable to each environment.

Acceptable Methods to Receive Payment

eCommerce Channel

- Customers submit payment through only approved eCommerce sites (i.e., honest.com, honestbeauty.com)

Client Services (Call Center)

- Employees can only accept payment information via phone call *(no credit card data can be requested by chat, email, sms, or other unapproved services for collection)*. Customer Service Representatives *must use only approved software/services* to assist customers with card-related issues (i.e., add new cards, replace expired cards, etc.). (*Currently Sandbox / Backend*)

Wholesale / Sales Operations / Business Development

- Employees accept only digital payments (*Currently DocuSign integrated with PayPal*)

Retail Channel

- Only approved hardware software and devices can be used (*currently Square*)

Employees must use only approved technologies for payment collection (*see above*) and not use any 3rd party payment related services unless they are explicitly approved.

Employees must only use company owned equipment when performing payment related work.

Employees that perform payment related functions are required to complete annual security training (*currently Wombat Security Training)*

Employees that are concerned or suspicious about credit card fraud and/or abuse should contact their management, Information security and/or Legal counsel.

Penalties for non- compliance with PCI

Fines up to $100,000 per month could be levied upon The Honest Company, Inc, as well as increased transaction fees or termination of use of the payment brand. Additionally, there could be significant impacts for brand reputation, breach related costs, and regulatory issues.

For any questions regarding this policy contact **security@honest.com**

Acknowledgment of Receipt of Compliance

I have received, reviewed, and understand the The Honest Company, Inc. Payment Card Industry Data Security Standard Policy and hereby undertake, as a condition to my present and continued employment at The Honest Company, Inc. to comply fully with the policies and procedures contained therein.

Signature Date Date

Printed Name