



STATE OF NH
DEPT OF JUSTICE

2016 NOV 14 AM 10:49

November 9, 2016

Joshua A. James
Direct: (202) 508-6265
josh.james@bryancave.com

CONFIDENTIAL

VIA FEDERAL EXPRESS

State of New Hampshire Department of Justice
Office of the Attorney General Joseph Foster
33 Capitol Street
Concord, NH 03301

Re: Data Security Breach Voluntary Notification

To Whom It May Concern:

EILEEN FISHER, Inc. (“EILEEN FISHER”), a client of Bryan Cave LLP, is notifying the Office of the Attorney General that EILEEN FISHER is notifying 116 clients who reside in New Hampshire of a criminal cyber-attack on the EILEEN FISHER e-commerce site. This letter is being provided as a courtesy as we do not believe notification is required under N.H. Rev. Stat. 359-C:19.

In late October, EILEEN FISHER was made aware of a possible data security incident affecting its e-commerce website between September 7 and October 24, 2016. EILEEN FISHER immediately began investigating the incident and enlisted a leading forensics firm to help in its investigation.

While the investigation is ongoing, at this time EILEEN FISHER believes that malicious code was added to the EILEEN FISHER website which allowed unauthorized individuals to capture certain payment information during the checkout process. The information potentially affected includes customer name, shipping and billing address, and credit card number used to make a purchase on eileenfisher.com.

U.S. customers that made a purchase from the EILEEN FISHER website, and customers that began making a purchase but ultimately did not complete that purchase, may have been affected by this incident.

EILEEN FISHER has removed the malicious code and excluded the unauthorized individual from its website.

EILEEN FISHER has notified its payment processor. In addition, EILEEN FISHER is notifying all potentially affected customers on November 9, 2016 via email. An example of the customer message is attached (please note that two slightly different versions were sent depending on whether the customer completed a transaction or only began the order process but did not complete the transaction). While it is unlikely that this event will result in new account creation identity theft, EILEEN FISHER is offering each affected customer a one-year subscription to two AllClear ID services that are focused on identifying or remediating existing account fraud that might impact the credit card accounts involved:

AllClear Identity Repair: This service is automatically available to customers with no enrollment required. If a problem arises, a customer may simply call 855.231.9570 and a dedicated investigator will help them recover financial losses, restore their credit and make sure their identity is returned to its proper condition.

AllClear Identity Theft Monitoring: AllClear, working in partnership with the National Cyber-Forensics and Training Alliance (NCFTA), which runs a global clearinghouse for stolen credentials, will alert customers about potentially compromised data, including credit card numbers. When AllClear receives data from the NCFTA that matches a customer's data, AllClear will alert the customer. This service also offers \$1 million identity theft insurance coverage.

Information regarding these services, as well as additional information to assist customers, is included in the notification sent to the customer.

If you would like any additional information concerning the above event, please feel free to contact me at your convenience.

Sincerely,

/s/ Joshua James

Joshua James

Attachment