BRYAN CAVE

BRYAN CAVE LLP 1155 F Street, N.W., Washington, D.C. 20004-1357
T: 202 508 6000 F: 202 508 6200 bryancave.com

November 9, 2016

Joshua A. James
Direct: 202/508-6265
Fax: 202/220-7565
josh.james@bryancave.com

**CONFIDENTIAL**

**VIA EMAIL**

Oregon

Re: Voluntary Data Security Breach 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 359 clients who reside in Oregon 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 ORS 646A.600.

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

# ATTACHMENT

To: [Customer]
From: [CEO]

Subject Line: Important Notice from EILEEN FISHER, Inc.

**Notice of Data Breach**

Dear [First Name],

For over 30 years, we have strived to uphold the highest standards of security, trust and transparency in the relationship with our customers. It is our company ethos to maintain and pursue exemplary business practices to better serve our community.

**What Happened**
Our records show that you made a purchase on eileenfisher.com between Wednesday, September 7 – Monday, October 24, 2016. In late October, we were informed of a possible data security incident that affected our website during that time.

We immediately began investigating the situation and are working diligently with a leading forensics firm to explore the issue. At this time, we believe that malicious code was added to our website which allowed unauthorized individuals to capture certain information during the checkout process. We have removed that malicious code and excluded the unauthorized individuals from our website.

**What Information Was Involved?**
While the investigation is still ongoing, we have confirmed the possibility that unauthorized individuals may have gained access to your name, the shipping and billing address, and the credit card number used to make your purchase on eileenfisher.com.

**What We Are Doing**
The security of our customers' information is always a priority and we sincerely regret any inconvenience to you.

As an added precaution, we have arranged to have AllClear ID assist customers with AllClear's Identity Repair and Identity Theft Monitoring services for 12 months at no cost to you. You can find more details about the services below.

**What You Can Do**
While this investigation is still underway, no matter what the outcome, please note the following:

- You have zero liability for any charges that you didn't make.
- Sign up for AllClear Identity Theft Monitoring services (explained below).
- Be wary of telephone or email scams.

**For More Information**

As part of our effort to provide you with timely, accurate information, we have enlisted the help of AllClear ID's Identity Protection Support Services. They can be reached at 855.231.9570 and will provide you with answers to your questions or will find the appropriate person who can answer your questions.

For more information and answers to frequently asked questions, please visit eileenfisher.com/info. This page will continue to be updated as we are committed to addressing your questions as quickly and accurately as possible.

Please know that no email from us will request personal information from you. If you receive an email that appears to be from EILEEN FISHER that requests personal information, please do not reply to that email; it is likely to be a scam.

We value your cooperation and patience as we investigate this incident.

SIGNED – Eileen
EILEEN FISHER, Founder and Chairwoman

**AllClear ID Services Available to You:**

**AllClear Identity Repair**: This service is automatically available to you with no enrollment required. If a problem arises, simply call 855.231.9570 and a dedicated investigator will help recover financial losses, restore your credit and make sure your 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 you about potentially compromised data, including credit card numbers. When AllClear receives data from the NCFTA that matches your data, AllClear will alert you. This service also offers $1 million identity theft insurance coverage.

To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 855.231.9570 using the following redemption code {Redemption_Code}.

Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

**Information about Identity Protection**

We recommend you remain vigilant with respect to reviewing your account statements, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC").

Although the information involved in this incident is unlikely to lead to the creation of new accounts using your identity, we recommend that, as a general matter, you regularly review statements from your accounts and periodically

obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

| | |
|---|---|
| **Equifax:** | P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com |
| **Experian:** | P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com |
| **TransUnion:** | P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com |

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Additionally, if you believe that you have been the victim of identity theft, you have the right to file a police report regarding that incident and obtain a copy of that police report. You may also obtain a police report regarding this incident if any is filed.

**Fraud Alerts:** There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

| | |
|---|---|
| Equifax: | 1-888-766-0008, www.equifax.com |
| Experian: | 1-888-397-3742, www.experian.com |
| TransUnion: | 1-800-680-7289, fraud.transunion.com |

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company (in Massachusetts, the fee is $5). *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

| | |
|---|---|
| Equifax: | P.O. Box 105788, Atlanta, GA 30348, www.equifax.com |
| Experian: | P.O. Box 9554, Allen, TX 75013, www.experian.com |
| TransUnion LLC: | P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com |

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

If you are a resident of Maryland or North Carolina, you can obtain additional information for how to avoid identity theft (including how to place a fraud alert or security freeze on your account) and how to report identity theft from the following sources:

| | |
|---|---|
| MD Attorney General's Office<br>Consumer Protection Division<br>200 St. Paul Place<br>Baltimore, MD 21202<br>1-888-743-0023<br>www.oag.state.md.us | NC Attorney General's Office<br>Consumer Protection Division<br>9001 Mail Service Center<br>Raleigh, NC 27699-9001<br>1-877-566-7226<br>http://www.ncdoj.gov/ |

## AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you—ever. AllClear Identity Repair is paid for by the participating Company.

**Services Provided**

If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

**Coverage Period**

Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that occurred prior to your Coverage Period are not covered by AllClear Identity Repair services.

**Eligibility Requirements**

To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

**How to File a Claim**

If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

**Coverage under AllClear Identity Repair Does Not Apply to the Following:**

Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

**Other Exclusions:**

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

**Opt-out Policy**

If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

| **E-mail** | **Mail** | **Phone** |
|---|---|---|
| support@allclearid.com | AllClear ID, Inc.<br>823 Congress Avenue Suite 300<br>Austin, Texas 78701 | 1.855.434.8077 |