

# **EXHIBIT 1**

The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Eileen Fisher, Inc. (“Eileen Fisher”) does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

### **Nature of the Data Event**

On or about October 14, 2021, Eileen Fisher learned of suspicious activity on its computer network. Eileen Fisher immediately secured its network and launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the incident. The investigation determined that certain files on Eileen Fisher’s systems that contain information related to employees and former employees may have been subject to unauthorized access and/or acquisition between July 2, 2021 and October 19, 2021.

Eileen Fisher began notifying individuals as information became available beginning on December 23, 2021. On or around January 5, 2023, Eileen Fisher completed its most recent review effort and determined that the information that could have been subject to unauthorized access includes name and Social Security number.

### **Notice to Maine Residents**

On or about March 1, 2023, Eileen Fisher provided written notice of this incident to three (3) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Eileen Fisher moved quickly to investigate and respond to the incident, assess the security of Eileen Fisher systems, and identify potentially affected individuals. Eileen Fisher is also working to implement additional safeguards and training to its employees. Eileen Fisher is providing access to credit monitoring services for 24 months, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals. Finally, Eileen Fisher reported the incident to law enforcement and is cooperating with the investigation.

Additionally, Eileen Fisher is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Eileen Fisher is providing individuals with information on how to place a fraud alert and security freeze on one’s credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Eileen Fisher is providing written notice of this incident to relevant state regulators, as necessary.

# **EXHIBIT A**

# EILEEN FISHER

<<Date>> (Format: Month Day, Year)

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

## <<b2b\_text\_1 (“NOTICE OF” [variable header])>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>,

Eileen Fisher, Inc. (“Eileen Fisher”) is writing to make you aware of an incident that may affect the security of some of your information. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident, our ongoing response, and resources available to you right now to help protect your information, should you feel it is appropriate to do so.

**What Happened?** On October 14, 2021, Eileen Fisher learned of suspicious activity on its computer network. We immediately secured our network and launched an investigation with the assistance of third-party computer specialists to determine the nature and scope of the incident. The investigation determined that there was unauthorized access to certain employee email accounts from on or around July 2, 2021 until October 19, 2021. We reviewed these accounts, and we determined that the accessed emails and attachments contained information relating to individuals. The investigation could not confirm what specific information within the accounts may have been accessed by the unauthorized individual. Therefore, in an abundance of caution, we undertook a diligent and comprehensive review of the entire contents of the impacted accounts to determine the information present in the accounts and potentially subject to unauthorized access. This resulted in the determination that your information was included in the impacted accounts. We then reviewed our records to identify contact information for potentially impacted individuals in order to provide this notice. On January 5, 2023, we completed our review. While there is no indication that your specific information was accessed or misused, in an abundance of caution we are notifying you now about the incident and the services available to you that are detailed below.

**What Information Was Involved?** The information that may have been impacted by this incident includes your <<b2b\_text\_2 (“name” and data elements)>>.

**What We Are Doing.** Eileen Fisher takes this incident and security of your information seriously. Upon discovering this incident, we immediately took steps to review and reinforce the security of our computing environment. We are reviewing our security policies, procedures, and processes, adding to our security systems, and rolling out additional workforce training to reduce the likelihood of a similar future incident. We have reported the incident to law enforcement and are cooperating with their investigation. We will also notify applicable regulatory authorities, as required by law.

As an added precaution, we are also offering twenty-four (24) months of complimentary access to identity monitoring services through Kroll, which includes Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. Individuals who wish to receive these services must activate by following the activation instructions found in the enclosed *Steps You Can Take to Help Protect Personal Information*.

**What You Can Do.** We encourage you to remain vigilant against identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to help protect your information in the enclosed *Steps You Can Take to Help Protect Personal Information*. There you will also find more information on the identity monitoring services we are offering and how to activate.

**For More Information.** We understand you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call us at [xxx-xxx-xxxx](tel:xxx-xxx-xxxx), Monday through Friday between the hours of 8:00 a.m. and 5:30 p.m. Central Time, excluding some major U.S. holidays.

Sincerely,

A handwritten signature in cursive script that reads "Carol Massoni".

Carol Massoni  
Eileen Fisher, Inc.

## STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

### **Activate Your Identity Monitoring Services**

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for twenty-four (24) months. Kroll is a global leader in risk mitigation and response, and its team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until <<b2b\_text\_6 (activation date)>> to activate your identity monitoring services.*

Membership Number: <<Activation Code s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

You have been provided with access to the following services from Kroll:

#### **Triple Bureau Credit Monitoring**

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

#### **Fraud Consultation**

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

#### **Identity Theft Restoration**

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

### **Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;

3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

| <b>Equifax</b>                                                                                                                  | <b>Experian</b>                                                             | <b>TransUnion</b>                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a> | <a href="https://www.experian.com/help/">https://www.experian.com/help/</a> | <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045                                                                                                                  | 1-888-397-3742                                                              | 1-800-916-8800                                                                              |
| Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069                                                                     | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013                        | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016                                    |
| Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788                                                                   | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013                      | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094                                   |

### **Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

*For District of Columbia residents*, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and [oag.dc.gov](http://oag.dc.gov).

*For Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us). Eileen Fisher, Inc. is located at 2 Bridge Street, Suite 230, Irvington, NY 10533.

*For New Mexico residents*, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

*For New York residents*, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).