Abercrombie & Fitch

April 15, 2015

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

Re: Notification of Security Incident

Dear Sir or Madam:

We are writing to inform you of a recent security incident involving Abercrombie & Fitch ("Abercrombie"), headquartered in New Albany, Ohio. Abercrombie has recently learned that some of its employees' accounts on a self-help human resource portal were accessed by another individual using the employees' usernames and passwords. There is no indication that the employees' login and password were obtained from the Abercrombie systems. This individual changed the employees' email addresses and direct deposit information in an attempt to divert their direct deposits. All employees have been fully paid and did not suffer a pay loss as a result of this event. Based on Abercrombie's investigation, it has not been determined that any other personal information in the employees' accounts was accessed, or of any misuse of other employee personal information. We have notified the FBI of the attempted theft.

At this time it is believed that approximately 1 Abercrombie employee in your state was potentially affected. We sent the enclosed letter to the affected individual in your state on April 15, 2015.

Sincerely,

[redacted]

Enclosure

[redacted]

Via Overnight Delivery

April 15, 2015

Name
Address
City, State zip

Dear (Name),

Re: Notification of Security Incident

On Friday April 10, 2015 we learned that an individual accessed your account on my.anfcorp.com using your login and password. Once accessed, this individual changed your email address and direct payroll deposit information in an attempt to divert the direct deposit to a different bank account. We took immediate steps to isolate this incident and correct your payroll deposit information and notified the FBI of the attempted theft.

There is no indication that your login and password were obtained from the Abercrombie systems. As a precaution, we have locked your login account. You will be required to change your password the next time you come into work. Please speak to your Manager for help in doing so. Your new password should be a strong password, with no less than 8 digits. When you change your password, please also change your e-mail address and verify that your personal information, including your bank account, is correct.

Based upon the information from our investigation, it appears that the changes to your direct deposit and e-mail information in your my.anfcorp.com account occurred on or around late March 2015. We have included with this letter further information on how you can protect yourself in the event other information in your my.anfcorp.com account was acquired and misused. In addition, we will be providing you with one year of monitoring, at no cost to you, from All Clear ID. You may sign up online at **enroll.allclearid.com** using the following redemption code: INSERT CODE, beginning immediately.

Please contact us at 614.765.5548 if you have additional questions.

Sincerely,

John Gabrielli
Senior Vice President, Human Resources

Enclosure

Further Information and Steps You Can Take

Information from the Federal Trade Commission

The Federal Trade Commission provides suggestions for actions in the event of identity theft, including information about fraud alerts and security freezes, at http://www.consumer.ftc.gov/features/feature-0014-identity-theft. You may also contact the Federal Trade Commission for more information toll-free at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Obtaining a free credit report or placing a fraud alert or security freeze

You may obtain a free copy of your credit report from each of the credit bureaus once a year by going to http://www.annualcreditreport.com or calling 877-322-8228. Hearing impaired consumers can access TDD services at 877-730-4104. We encourage you to vigilantly monitor these reports, as well as your credit and debit card statements. You may also place a fraud alert or security freeze on your credit report by contacting the credit bureaus as listed below.

Equifax	Experian	TransUnion
P.O. Box 740241	P.O. Box 9554	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
888-766-0008	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

A security freeze will prevent new credit from being opened in your name without the use of a personal identification number or password that will be issued by the credit bureaus after you initiate the freeze. A security freeze will also prevent potential creditors from accessing your credit report without your authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. In order to place a security freeze, you may be required to provide the credit bureaus with information that identifies you, including your full name, social security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. Credit bureaus may charge a fee up to $10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to $5) or waived if you are the victim of identity theft and you provide a valid police report. You must separately place a security freeze on your credit file with each credit reporting agency.

Filing a Police Report for Suspicious Activity

If you do find suspicious activity on the credit or debit card indicated in our notice to you or in your credit report, call your local police or sheriff's office and file a police report of identity theft. Get a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. In addition, you should report identity theft to your Attorney General and the Federal Trade Commission.

For Maryland Residents: The Maryland Attorney General provides information regarding identity theft at http://www.oag.state.md.us/idtheft/index.htm. You may also contact the Identity Theft Unit at (410) 576-6491, by email at idtheft@oag.state.md.us, and by mail at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

For North Carolina Residents: The North Carolina Attorney General provides information about avoiding identity theft at http://www.ncdoj.com. You may also contact the North Carolina Department of Justice at (877) 566-7226, or by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001.

For Iowa Residents: The Attorney General provides information about preventing identity theft at http://www.iowaattorneygeneral.gov. You may also contact the Iowa Attorney General by calling (515) 281-5164, or by mail at 1305 E. Walnut Street, Des Moines, IA 50319.