BakerHostetler

Baker&Hostetler LLP
2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891
T 215.568.3100
F 215.568.3439
www.bakerlaw.com
Anthony P. Valach
direct dial: 215.564.2588
avalach@bakerlaw.com

October 5, 2018

Via overnight mail

Gordon MacDonald
Office of the Attorney General
33 Capitol St.
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Five Below, Inc. ("Five Below"), to notify you of a security incident involving 13 New Hampshire residents.

On August 28, 2018, Five Below's security team observed suspicious activity on its website. Five Below immediately began an investigation with the assistance of a leading computer security firm. On September 10, 2018, the investigation identified the potential for unauthorized access to payment card data. Findings from the investigation suggest that certain customers' order information and payment card information, including name, address, payment card number, expiration date, and card security code (CVV), may have been obtained by an unauthorized third party. This incident involved 13 residents of New Hampshire who placed or attempted to place orders on Five Below's website between August 14, 2018 and August 28, 2018 or between September 18, 2018 and September 19, 2018. Purchases made in Five Below stores were not involved in this incident. To date, Five Below is not aware of any misuse of the information or any other criminal activity as a result of the incident.

On October 5, 2018, Five Below will begin mailing notification letters to 13 New Hampshire residents in accordance with N.H. Rev. Stat. Ann. § 359-C:20 via United States First-Class mail, in substantially the same form as the enclosed letter. Notice is being provided to the individuals as soon as possible and without undue delay. Five Below is providing a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent a similar incident from occurring in the future, Five Below has further enhanced the security measures for its website. In addition, Five Below is working with the payment card networks so that banks that issue payment cards can be made aware.

Five Below takes the security of its customers' personal information very seriously and is committed to protecting customers' personal information. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

Anthony P. Valach
Counsel

Enclosure

five BELOW®

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear <<Name 1>>:

Five Below, Inc. ("Five Below") understands the importance of protecting the payment card information of our customers. We are writing to inform you of a recent incident that may have involved that information. This letter explains the incident, measures we have taken, and steps you can take in response.

On August 28, 2018, our security team observed suspicious activity on our website. We immediately began an investigation with the assistance of a leading computer security firm. On September 10, 2018, the investigation identified the potential for unauthorized access to payment card data. Findings from the investigation suggest that certain of our customers' order information and payment card information, including name, address, payment card number, expiration date, and card security code (CVV), may have been obtained by an unauthorized third party. We believe the incident only involved customers who placed or attempted to place orders on our website between August 14, 2018 and August 28, 2018 or between September 18, 2018 and September 19, 2018. We are notifying you because you placed or attempted an order on www.fivebelow.com during those time periods using a payment card ending in **<<variable data>>**. Purchases made in our stores were not affected by this incident.

We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card because payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. The phone number to call is usually on the back of your payment card.

To date, we have no information that any of your personal information was misused in any way. As a precaution, we have secured the services of Experian to offer you a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with identity detection and resolution of identity theft services. For more information on IdentityWorks℠, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take to protect yourself, please see the pages that follow this letter.

We take the security of our customers' personal information very seriously. To help prevent a similar incident from occurring in the future we have further enhanced the security measures for our website. In addition, we are working with the payment card networks so that banks that issue payment cards can be made aware.

If you have any questions, please call 877-861-1227, Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern Time.

Sincerely.

David Makuen
Executive Vice President, E-Commerce

ACTIVATE YOUR 12 MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-888-397-3742. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

To activate your membership and start monitoring your personal information please follow the steps below:

This product provides you with internet surveillance, and identity theft insurance at no cost to you upon enrollment.

- Ensure that you **enroll by**: **<<enrollment end date>>** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/identity
- Provide your **activation code**: **<<code>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-888-397-3742 by **<<enrollment end date>>.** Be prepared to provide engagement number **<<engagement #>>** as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you detect any unauthorized activity on financial accounts, you should immediately contact your financial institution. We also recommend that you make your financial institution aware of this incident and take their advice on steps to protect your bank account. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, North Carolina, you may contact and obtain information from your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 860-808-5318, www.ct.gov/ag

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 888-743-0023 (toll free when calling within Maryland), (410) 576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 919-716-6400

Credit Freezes: You have the right to put a "security freeze," also known as a credit freeze, on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security 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 security 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 have the right to freeze and unfreeze your credit report free of charge with the three credit reporting agencies. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.

For more information, visit the FTC's identity theft website at www.identitytheft.gov. To place a security freeze on your credit report, you can submit a request on the websites of the three major reporting agencies or send a written request to each by regular, certified, or overnight mail at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com
Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic system maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic system maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one (1) business day after receiving your request by toll-free telephone or secure electronic means, or three (3) business days after receiving your request by mail, to remove the security freeze.

Fraud Alerts: As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your 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 7 years.

For more information, visit the FTC's identity theft website at www.identitytheft.gov. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Fair Credit Reporting Act: You also have rights under the federal Fair Credit Reporting Act, which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Experian, TransUnion and Equifax – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like denying your application for credit, insurance, or employment, and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.