

AG CONSUMER [AG]

From: Hoar, Sean <SeanHoar@dwt.com>
Sent: Thursday, August 18, 2016 7:41 PM
To: AG CONSUMER [AG]
Cc: Folkestad, Vicki
Subject: Security Incident Notice
Attachments: IA AG Notification EB.PDF; Eddie Bauer non-Massachusetts consumer notification final.PDF

Dear Attorney General Miller: I represent Eddie Bauer, LLC, headquartered in Bellevue, Washington. This letter is being sent pursuant to Iowa Code §§ 715C.1-2 because Eddie Bauer determined on August 11, 2016 that 19,672 residents of Iowa may have had their payment card information affected by an information security incident. Eddie Bauer is in the process of notifying all affected consumers with the attached letter. Please contact me should you have any questions or require further information. Thanks. Sean.

Sean B. Hoar, CISSP, CIPP/US | Davis Wright Tremaine LLP
1300 SW Fifth Avenue, Suite 2400 | Portland, OR 97201
Tel: 503.778.5396 | Fax: 503.778.5299 | Mobile: 503.459.7707
Email: seanhoar@dwt.com | Website: www.dwt.com
Toll Free 24-Hour Data Breach Hotline 844.468.6398
Data Breach Team email DWTBreach@dwt.com

Anchorage | Bellevue | Los Angeles | New York | Portland | San Francisco | Seattle | Shanghai | Washington, D.C.



DAVIS WRIGHT TREMAINE
**"Innovative Law
Firm of the Year"**

August 18, 2016

Iowa Attorney General Tom Miller
Consumer Protection Division
ATTN: Security Breach Notifications
Office of the Attorney General of Iowa
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319

Re: Security Incident Notice

Dear Attorney General Miller:

I represent Eddie Bauer, LLC, headquartered in Bellevue, Washington. This letter is being sent pursuant to Iowa Code §§ 715C.1-2 because Eddie Bauer determined on August 11, 2016 that 19,672 residents of Iowa may have had their payment card information affected by an information security incident.

Eddie Bauer determined that its retail store point of sale systems may have been accessed without authorization on July 15, 2016, but due to the sophistication of the attack and the complexity of the forensics investigation, we were not able to determine the identity of the affected cardholders until August 11, 2016. As soon as Eddie Bauer learned that its systems were affected, it engaged a digital forensics firm to investigate the matter. The investigation discovered that its point of sale systems were targeted by sophisticated malware that had also targeted restaurants, hotels, and other retailers. Payment card information used for online purchases at eddiebauer.com was not affected.

We are working closely with the FBI to identify the perpetrator(s), and will provide whatever cooperation is necessary to do so. We also notified the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the timeframe in which cards may have been compromised. We have also enhanced the security of our point of sale systems, with the goal of making it more difficult for a similar incident to occur in the future.

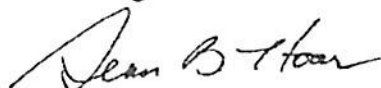
Eddie Bauer is in the process of notifying all affected consumers with the attached letter. As referenced in the letter, they will provide 12 months of credit monitoring and identity protection services to affected consumers through Kroll.

August 18, 2016
Page two

Please contact me should you have any questions.

Sincerely,

Davis Wright Tremaine LLP

A handwritten signature in black ink that reads "Sean B. Hoar". The signature is written in a cursive style with a large initial "S" and a long horizontal stroke at the end.

Sean B. Hoar

cc: Domenick Gallo, General Counsel
Eddie Bauer, LLC



August 18, 2016

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

Subject: Notice of Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to inform you of a data security incident that may have involved your payment card information. We take the privacy and security of your information very seriously. This is why we are contacting you, offering you identity protection services, and informing you about steps that can be taken to protect your payment card information.

What Happened? We recently learned that point of sale systems at Eddie Bauer retail stores may have been accessed without our authorization. We immediately initiated a full investigation with third-party digital forensic experts. On August 11, 2016 we received confirmation that your payment card information used at one or more of our retail stores (payment card ending in <<ClientDef1(Payment Card Number)>>) may have been accessed without authorization. This may have occurred on various dates between January 2, 2016 and July 17, 2016. Not all cardholder transactions during this period were affected, but out of an abundance of caution, we are notifying you of the incident and offering you identity protection services. Payment card information used for online purchases at eddiebauer.com was not affected.

What Information Was Involved? The information included your name, payment card number, security code and expiration date.

What Are We Doing? We are notifying you of the incident and are providing you information about the steps you can take to protect your payment card information. We have also arranged to have Kroll, a global leader in risk mitigation and response, provide you complimentary services for 12 months. We are also working closely with the FBI to identify the perpetrator(s), and will provide whatever cooperation is necessary to do so. We also notified the payment card networks so that they can coordinate with card issuing banks to monitor for fraudulent activity on cards used during the timeframe in which cards may have been compromised. Finally, the security of our point of sale systems has been enhanced, with the goal of making it more difficult for a similar incident to occur in the future.

What You Can Do: You can follow the recommendations on the following pages to protect your personal information. You can also enroll in the services we are offering through Kroll, at no cost to you. 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. Your services start on the date of this notice and can be used at any time during the next 12 months. They will include credit monitoring and identity consultation and restoration. Visit <https://kroll.idMonitoringService.com> to take advantage of these services. Your membership number is <<Member ID>>. To receive credit services by mail instead of online, please call 1-855-294-2549. Additional information describing your services is included with this letter.

For More Information: Further information about how to how to protect your personal information appears on the following pages. If you have questions or need assistance, call 1-855-294-2549, 8:00 a.m. to 5:00 p.m. (Central Time), Monday through Friday. Kroll's licensed investigators are standing by to assist you. Please have your membership number ready.

Protecting our customers' personal information – and maintaining your trust – is of paramount importance to Eddie Bauer. We sincerely apologize for any inconvenience this incident has caused you.

Sincerely,

A handwritten signature in black ink, appearing to read "Mike Egeck". The signature is fluid and cursive, with the first name "Mike" and last name "Egeck" clearly distinguishable.

Mike Egeck
Chief Executive Officer
Eddie Bauer

Information about Protecting Personal Information

Review Your Account Statements and Notify Issuing Bank & Law Enforcement of Suspicious Activity: It is recommended that you remain vigilant for any incidents of fraud or identity theft by regularly reviewing credit card account statements and your credit report for unauthorized activity. If you detect any suspicious activity on an account, we recommend you contact your issuing bank immediately to either freeze or close the account. You may also report any fraudulent activity or any suspected identity theft to local law enforcement, the Federal Trade Commission (FTC), or your respective state Attorney General. Residents of Massachusetts and Rhode Island have the right to obtain any police report filed in regard to this incident.

Copy of Free Credit Report: You may obtain a free copy of your credit report from the following national consumer reporting agencies or from the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281, 1-877-322-8228, www.annualcreditreport.com:

Equifax: P.O. Box 105139, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com

Experian: P.O. Box 2002, Allen, TX 75013, 1-888-397-3742, www.experian.com

TransUnion: P.O. Box 6790, Fullerton, CA 92834-6790, 1-800-916-8800, www.transunion.com

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, the **FTC**, or your respective state Attorney General about steps you can take toward preventing identity theft. The FTC may be contacted at **FTC, Consumer Response Center**, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-438-4338, www.ftc.gov/idtheft.

For residents of Maryland, North Carolina, and Rhode Island: Residents of Maryland, North Carolina and Rhode Island can also obtain information about preventing and avoiding identity theft from their attorneys general at the addresses below, and from the Federal Trade Commission.

Maryland Office of the
Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

North Carolina Office of the
Attorney General
Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

Rhode Island Office of the
Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
<http://www.riag.ri.gov>

Fraud Alerts: There are 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 consumer reporting agencies listed below:

Equifax: 1-800-525-6285, www.equifax.com

Experian: 1-888-397-3742, www.experian.com

TransUnion: 1-800-680-7289, www.transunion.com

Credit Freezes (for Non-Massachusetts Residents): 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 agency. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency 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. Since the instructions for how to

establish a credit freeze differ from state to state, please contact the three major consumer reporting agencies 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: P.O. Box 2000, Chester, PA, 19022-2000, www.transunion.com

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



TAKE ADVANTAGE OF YOUR COMPLIMENTARY SERVICES

You've been provided with access to the following services¹ from Kroll:

Credit Monitoring through TransUnion

You'll 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 investigator, who can help you determine if it's an indicator of identity theft.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to 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 Restoration

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

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

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.