WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK
DIRECT LINE (410) 832-2002
DIRECT FAX (410) 339-4028
spollock@wtplaw.com

TOWSON COMMONS, SUITE 300
ONE WEST PENNSYLVANIA AVENUE
TOWSON, MARYLAND 21204-5025
MAIN TELEPHONE (410) 832-2000
FACSIMILE (410) 832-2015

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

Certified Article Number
9414 7266 9904 2129 2367 09
SENDER'S RECORD

August 5, 2021

Privileged and Confidential
VIA EMAIL AND FIRST CLASS MAIL
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Security Breach Notification

Dear Commissioner Little,

We are writing on behalf of our client, Ski Bromley, LLC d/b/a Bromley Mountain Ski Resort, a subsidiary of Belmont Navy LLC ("Bromley") (located at 55 Cambridge Parkway, Suite 200 Cambridge, MA 02142 and authorized to do business at 3984 Vermont Route 11, Peru, VT), to notify you of a data security incident involving eleven (11) New Hampshire residents.[1]

Nature

On June 28, 2021, Bromley discovered that they were the victim of a sophisticated ransomware attack that resulted in encryption and unauthorized access to their network. At that time, Bromley took immediate steps to stop the threat and understand the full scope of the situation. This included hiring third-party forensic experts to conduct a thorough investigation and remediation efforts. On July 7, 2021, Bromley retrieved and confirmed the deletion of the information obtained by the unauthorized individual to the best of their ability. On July 28, 2021, Bromley concluded its investigation and found that the unauthorized individual gained access to its systems via a firewall vulnerability. Further, after concluding a comprehensive review of the potentially impacted data, Bromley believes that the incident could have involved personal information related to eleven (11) New Hampshire residents. The personal information potentially included social security numbers.

[1] By providing this notice, Bromley does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Notice and Bromley's Response to the Event

On August 6, 2021, Bromley will mail a written notification to the potentially affected New Hampshire residents, pursuant to N.H. Rev. State § 359-C:19, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, Bromley is providing these potentially impacted individuals the following:

- Free access to credit monitoring services for at least one year, through Sontiq;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank.
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- 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 and law enforcement to report attempted or actual identity theft and fraud.

Further, Bromley provided the notice to the three major credit reporting agencies along with the applicable government regulators, officials, and other Attorney Generals (as necessary).

Finally, Bromley is working to implement any necessary additional safeguards, enhance and improve its policies and procedures related to data protection, improve its cybersecurity infrastructure, and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-2002 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

<Return Name>
<Return Address>
<City> <State> <Zip>

Ski Bromley, LLC
(d/b/a Bromley Mountain Ski Resort,
a subsidiary of Belmont Navy LLC)
3984 Vermont Route 11
Peru, VT 05152
802.824.5522

<FirstName> <LastName>
<Address1>
<Address2>
<City>, <State> <Zip>

[Date]

Re: Notice of Data Breach

Dear <First Name> <Last Name>,

We are writing to notify you of a recent incident involving Ski Bromley, LLC's network that may have impacted some of your personal information. As such, we are providing you with background about the incident, what we did in response, and steps you can take to protect yourself against possible misuse of your personal information.

What Happened

On June 28, 2021, we discovered that we were the victim of a sophisticated ransomware attack that resulted in encryption and unauthorized access to our network, during the same week approximately 1500 other companies may have experienced a ransomware compromise. At that time, our firm took immediate steps to stop the threat and understand the situation's full scope. After concluding our initial forensic investigation, we determined that the unauthorized individual acquired some of the information contained on our systems. Further, on July 7, 2021, we retrieved and confirmed the deletion of the information obtained by the unauthorized individual to the best of our ability. On July 29, 2021, we concluded our comprehensive review of the potentially impacted data and believe that your information could have been involved in the incident. As of now, we have no evidence indicating any misuse of your information, but out of an abundance of caution and complete transparency, we wanted to notify you about this incident.

What Information Was Involved

The information potentially includes your <specific personal information>.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. As such, we are working to implement any necessary additional safeguards by engaging external legal and cybersecurity experts to assist in this process, further training our employees, and reviewing and improving our internal procedures as necessary to minimize the likelihood of this type of incident occurring again.

Further, we are providing you with access to Single Bureau Credit Monitoring* for one year. These services provide you with alerts for one year from the date of enrollment when changes occur to your Experian credit file. We are providing this service free of charge, and signing up for this service will not impact your credit score. This product helps detect any potential misuse of your personal information and gives you identity protection services that will help with resolving and identifying any potential identity fraud or theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

To enroll in these services, please log on to https://www.myidmanager.com and follow the instructions provided. When prompted, please provide the following unique code to receive services: <access code>.

To receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

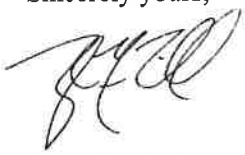
What You Can Do

We encourage you to review the enclosed ***Other Important Information,*** which contains essential information on how to best protect yourself from potential identity theft and fraud. Further, we strongly recommend you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement.

For More Information

We sincerely regret this incident, and we understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, please call our toll-free helpline response line at 1-800-405-6108 between 8:00 a.m. and 8:00 p.m. (EST) Monday – Friday.

Sincerely yours,



Tyler H. Fairbank, Manager

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age.
Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.

You can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Provided below are the three nationwide credit reporting agencies' contact information to request a copy of your credit report or general identified above inquiries.

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Security Freeze (also known as a Credit Freeze)

You have the right to put a credit or security freeze on your credit file. A security freeze makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze.

To place a request for a security freeze, you will need to provide some or all of the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail, including your (1) 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, the addresses of your previous addresses during that time, (5) proof of your current address (i.e., a current bill from your utility, cable, or telephone copy, rental agreement, deed, etc.), (6) a legible photocopy of a government-issued identification card (i.e., a state driver's license or ID card, military identification, passport, etc.), (7) social security card, pay stub or W2, and or (8) if you are a victim of identity theft and have a police report, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request 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), password, or both that you can use to authorize the removal or lifting of the security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Consider Placing a Fraud Alert on Your Credit Report

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified

above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338).

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf

Maryland residents may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **Massachusetts residents**: State law advises you that you have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). You also will not be charged for seeking a security freeze, as described above in this document. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at https://ncdoj.gov/protecting-consumers/identity-theft/, or by contacting the Attorney General by calling *1-877-566-7226* or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 9001 Mail Service Center Raleigh, NC 27699. Further, **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877- 9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. Alternatively, you can file a police report). Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services.