

November 1, 2023

Via Certified Mail; Return Receipt Requested:

Attorney General John M. Formella
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
603-271-3658
attorneygeneral@doj.nh.gov

RECEIVED
NOV 09 2023
CONSUMER PROTECTION

Re: Cybersecurity Incident Involving Mt. Hood Meadows Oreg LLC.

Dear Attorney General Formella:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Mt. Hood Meadows Oreg LLC ("Mt. Hood Meadows"), a Ski resort located in 14040 OR-35, Mt Hood, OR 97041, with respect to a recent cybersecurity incident that was first discovered by Mt. Hood Meadows on March 9, 2023 (hereinafter, the "Incident"). Mt. Hood Meadows takes the security and privacy of the information in its control very seriously, and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of New Hampshire residents being notified, and the steps that Mt. Hood Meadows has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On March 9, 2023, Mt. Hood Meadows Oreg LLC ("Mt. Hood Meadows") suspected unusual activity on its website. An unauthorized third party attempted to infiltrate Mt. Hood Meadows' network by way of code modification on the web server.

Upon discovery of this incident, Mt. Hood Meadows moved quickly to secure the network environment and launched a thorough investigation with the help of independent IT security and forensic investigators to determine the scope and extent of the potential unauthorized access to their systems and any personal information. The forensic investigation found some evidence that some client information may have been accessed by an unauthorized individual, revealing the possibility that users who made purchases from the Mt. Hood Meadows website from February

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

wilsonelser.com

21, 2023 through March 14, 2023 could have had their

Mt. Hood Meadows provided substitute notice on April 21, 2023.

2. Number of New Hampshire residents affected.

A total of 15 (fifteen) New Hampshire resident(s) may have been potentially affected by this incident. Notification letters to these individuals will be mailed on October 27, 2023. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Upon discovery of the incident, Mt. Hood Meadows moved quickly to investigate and respond to the incident, including taking down the website until they could ensure it was secure. Mt. Hood Meadows mitigated attempts to gain access to guest information. Mt. Hood Meadow's website was relaunched only when it could ensure the issue had been resolved.

Mt. Hood Meadows also immediately contacted the FBI to report the potential compromise. In the months since the incident, Mt. Hood Meadows has replaced their entire website partnering with Big Commerce, a leading E-commerce provider to ensure they are on a secure platform, and had a security audit of their network from CFC Response which identified no malware.

Mt. Hood Meadows has also reviewed and taken steps to enhance their policies and procedures relating to the security of their systems and servers, as well as information life cycle management. Mt. Hood Meadows has taken all efforts possible to mitigate any further exposure of personal information and related identity theft.

To help relieve concerns and restore confidence following this incident, Mt. Hood Meadows has secured the services of Kroll to provide identity monitoring at no cost to affected individuals for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

4. Contact information

Mt. Hood Meadows highly values the security of personal data. If you have any questions or need additional information, please do not hesitate to contact me at



Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

EXHIBIT A



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Via First-Class Mail

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Mount Hood Meadows Oregon, LLC ("Mount Hood") is writing to inform you of a data security incident that may have resulted in an unauthorized access to your sensitive personal information. We are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information. Please be assured Mount Hood takes the protection and proper use of your personal information very seriously.

What Happened

On March 9th Mt. Hood suspected that an unauthorized individual had potentially used its website to obtain credit card information. The unauthorized access was later confirmed on March 12th. An unauthorized third party attempted to infiltrate Mount Hood's network by way of code modification on the web server. Upon discovery of this incident, Mount Hood promptly engaged in a comprehensive forensic investigation to determine the nature and scope of the incident. That investigation concluded on July 26, 2023.

What Information was Involved

It is possible that users who made purchases using our website from February 21, 2023 through March 14, 2023 could have had their

What We are Doing:

We take our data responsibilities and protection of our guest data very seriously and we are sorry for any worry and inconvenience this news will cause. Upon discovery of the incident, Mt. Hood Meadows moved quickly to investigate and respond to the incident, including taking down the website until we could ensure it was secure. Mt. Hood Meadows mitigated attempts to gain access to guest information. Mt. Hood Meadow's website was relaunched only when we could ensure the issue had been resolved.

Mt. Hood Meadows also immediately contacted the FBI to report the potential compromise. In the months since the incident, we have replaced our entire website partnering with Big Commerce, a leading Ecommerce provider to ensure we are on a secure platform and had a security audit of our network from CFC Response which identified no malware.

We have also reviewed and have taken steps to enhance our policies and procedures relating to the security of our systems and servers, as well as our information life cycle management. We would like to reassure you that we have taken all efforts possible to mitigate any further exposure of your personal information and related identity theft, and we are committed to supporting you.

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 one year. Kroll is a global leader in risk mitigation and response, and their 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: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

More Information:

If you have questions, please call _____, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Mount Hood values the security of your personal data, and we apologize for any inconvenience that this incident has caused.

Sincerely,

Greg Pack
President/GM
he, him

Steps You Can Take Help Protection Your Information

Credit Reports: You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 1-800-349-9960 https://www.equifax.com/personal/credit-report-services/credit-freeze/	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion Security Freeze P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze
---	---	--

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with:

- Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);
- TransUnion (<https://www.transunion.com/fraud-alerts>); or
- Experian (<https://www.experian.com/fraud/center.html>).

A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

File Police Report: You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

FTC and Attorneys General: You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338), 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. This notice has not been delayed by law enforcement.

For Arizona residents, the Attorney General may be contacted at the Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, 1-602-542-5025.

For Colorado residents, the Attorney General may be contacted through Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000, www.coag.gov.

For District of Columbia residents, the Attorney General may be contacted at the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov.

For Illinois residents, the Attorney General can be contacted at 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov.

For Iowa residents, you can report any suspected identity theft to law enforcement or to the Attorney General.

For Massachusetts residents, it is required by state law that you are informed of your right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For Maryland residents, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.

For New Mexico residents, state law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You also 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 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; 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 violators. 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 at 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, you may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, and www.ncdoj.gov. You may also obtain information about steps you can take to prevent identify theft from the North Carolina Attorney General at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/protect-yourself-from-id-theft/>.

For Oregon residents, state law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For Rhode Island residents, this incident involves <<#>> individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

For Vermont Residents: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Single 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 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.