McGuireWoods LLP
Gateway Plaza
800 East Canal Street
Richmond, VA 23219-3916
Phone: 804.775.1000
Fax: 804.775.1061
www.mcguirewoods.com

Christel E. Harlacher
Direct: 804.775.4391

McGUIREWOODS

March 15, 2024

VIA FEDERAL EXPRESS
The Honorable John Formella
Office of the Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Notice of Data Breach

Dear Attorney General Formella:

I am writing on behalf of The Biltmore Company, LLC ("Biltmore" or the "Company"), with its headquarters located at One North Pack Square, Asheville, NC, 28801, to report a recent data breach. Biltmore's online store (biltmoreshop.com) is a website where consumers may purchase wine and retail products. On February 16, 2024, Biltmore was notified that an unauthorized party inserted malicious code into the application Biltmore uses to process orders from this online retail store. The application is hosted by a third-party vendor. Biltmore immediately engaged its incident response team, including an external forensics and cybersecurity firm, to support its investigation, defense, and recovery. Through these actions, Biltmore contained the incident as of February 23, 2024. A forensic investigation was then conducted that confirmed that an unauthorized malicious party acquired payment card information from individuals who made purchases in the impacted online retail store beginning on December 5, 2023. Over the past several weeks, Biltmore undertook an extensive review of the incident to ensure that the Company accurately report the affected categories of data and individuals. Biltmore's other technology systems, including those related to ticket sales, hotel stays, and in-person purchases made on-site at Biltmore properties, were *not* impacted by this incident. Please note, Biltmore is not aware of any misuse of the impacted information including identity theft, fraud, or financial losses resulting from this incident and this notice was not delayed by a law enforcement investigation.

The data exposed as a result of this incident included personal information of 38 New Hampshire residents. Formal, written notices will be sent to the impacted consumers by U.S. mail on March 15, 2024.

Biltmore has taken comprehensive actions to mitigate the incident, including notifying the FBI, successfully locking the unauthorized malicious party out of the impacted application, undertaking a full forensic investigation, and temporarily closing its online retail store. Biltmore has also taken numerous steps to remove the malicious code in the impacted application and is

completely replacing the transaction environment. In addition, the Company is offering the impacted consumers a complimentary membership to Equifax's Credit Watch™ Gold services, which includes credit monitoring, daily access to credit report, WebScan notifications, fraud alerts, Identity Restoration, and up to $1,000,000 of identity theft insurance coverage.

A copy of the template form of the notification letter that will be sent to the affected New Hampshire residents is included with this notice. As you will see, among other things, the letter (i) describes various steps that affected individuals can take to protect themselves, (ii) provides contact information for consumer reporting agencies and relevant governmental agencies, and (iii) provides enrollment information for of credit monitoring services, which the Company is offering to the affected individuals at no cost.

If you have any questions about the information provided in this letter, or this incident generally, please feel free to contact me at the email or phone numbers listed above.

Sincerely,

Christel E. Harlacher

Enclosure: Template Form Notification Letter

EXHIBIT A

BILTMORE®

1 North Pack Square
Asheville, NC 28801

March 15, 2024

00695-ADFFIN G0104 L001 AUTO *000001

[redacted]

RE: Notice of Data Breach

Dear [redacted],

I am writing on behalf of The Biltmore Company, LLC ("Biltmore" or the "Company") with important information about a data security incident involving our online retail store where we sell wine and other retail items. Biltmore takes the protection and proper use of your personal information very seriously. We are writing to share information about this incident, provide details about the steps we have taken in response to this incident, and to explain the steps you can take to protect your personal information. We are not aware of any misuse of your information at this time, but we write to you out of an abundance of caution.

What Happened:

Biltmore's online store (biltmoreshop.com) is a website where consumers may purchase wine and retail products. On February 16, 2024, Biltmore was notified that an unauthorized party inserted malicious code into the application Biltmore uses to process orders from this online retail store. The application is hosted by a third-party vendor. Biltmore immediately engaged its incident response team, including an external forensics and cybersecurity firm, to support its investigation, defense, and recovery. Through these actions, Biltmore contained the incident as of February 23, 2024. A forensic investigation was then conducted that confirmed that an unauthorized malicious party acquired payment card information from individuals who made purchases in our online retail store beginning on December 5, 2023. Over the past several weeks, we undertook an extensive review of the incident to ensure that we accurately report the affected categories of data and individuals. Biltmore's other technology systems, including those related to ticket sales, hotel stays, and in-person purchases made on-site at Biltmore properties, were ***not*** impacted by this incident. Please note, Biltmore is not aware of any misuse of your information including identity theft, fraud, or financial losses resulting from this incident and this notice was not delayed by a law enforcement investigation.

What Information Was Involved:

The incident involved your . The malicious actor was able to access the information as it was entered into the online store when you were making a purchase. Biltmore does not store your full payment card information.

What We Are Doing:

We have taken comprehensive actions to mitigate the incident, including notifying the FBI, successfully locking the unauthorized malicious party out of the impacted application, undertaking a full forensic investigation, and temporarily closing our online retail store. We have also taken numerous steps to remove the malicious code in the affected application and we are completely replacing the transaction environment.

To assist consumers who were affected by this incident, we have secured Equifax's Credit Watch™ Gold services to provide identity monitoring and additional services at no cost to you for . Equifax is an American multinational consumer credit reporting agency with extensive experience serving people who have sustained an unintentional exposure of confidential data.

Visit **www.equifax.com/activate** to activate and take advantage of your identity monitoring services.

You have until to activate your identity monitoring services.

Activation Code: [redacted]

Additional information describing your services is included with this letter.

What You Can Do:

Please review the "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your personal information, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. You should also report any suspected incident of identity theft to law enforcement, and you can obtain a copy of any resulting police report. If you do suspect that you have been the victim of identity theft, please notify your state Attorney General and the Federal Trade Commission.

For More information:

If you have questions, please call **844-673-5167**, Monday through Friday from 9 a.m. to 9 p.m. Eastern Time to speak with an Equifax specialist that Biltmore has retained to assist you. Please have your activation code ready.

We deeply regret any effect this incident may have on you. We have been working diligently to address this incident. Protecting personal information is very important to us and we are committed to providing you with services to address this matter.

We sincerely apologize for any inconvenience it may cause you.

Sincerely,

Timothy Rosebrock
Vice President Compliance & Legal Services

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity or errors, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual 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 from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, and New Jersey residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

For New Mexico residents: You 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 bureaus 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 receive 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 by visiting 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.

Fraud Alerts. There are two types of fraud alerts 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have 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 contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. 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 may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, 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 5 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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 or 1-410-528-8662. The Biltmore Company, LLC is located at 1 North Pack Square Asheville, NC 28801.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226, 1-877-5-NO-SCAM, or 1-919-716-6000.

For Rhode Island residents: This incident impacted four (4) Rhode Island residents. You may contact the RI Office of the Attorney General, 150 South Main Street, Providence, RI 02903, (401) 274-4400; http://www.riag.ri.gov/ConsumerProtection/About.php# Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

For Washington D.C. residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and https://oag.dc.gov/

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

EQUIFAX®

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to **www.equifax.com/activate**

Enter your unique Activation Code then click "Submit"

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

You're done!

The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1] *WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.*

[2] *The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.*

[3] *Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com*

[4] *The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.*