CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

January 30, 2023

VIA E-MAIL

Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301
Doj.cpb@doj.nh.gov

Re: Notice of Data Security Incident

To Whom It May Concern:

We represent Vice Media LLC ("Vice"), a digital media and broadcasting company. Vice is headquartered in Brooklyn, New York. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19, C:20, C:21, because the personal information of four (4) New Hampshire residents may have been affected by a recent data security incident. The incident may have included unauthorized access to personal information such as names and Social Security numbers.

On or around March 29, 2022, Vice was alerted to unusual activity within its digital environment when 105 emails were sent out from what appeared to be an internal Vice account between March 29, 2022 and April 4, 2022. Upon discovering this activity, Vice immediately took steps to secure its network. Vice also engaged leading cybersecurity firms to conduct an investigation to determine what happened and whether personal information hosted on its network may have been involved. The investigation revealed that there may have been unauthorized access to an internal Vice e-mail account. Following a thorough review of the information contained in the email account, we determined that personal information may have been contained within the account. We then worked to obtain up-to-date addresses for individuals whose personal information may have been involved which was completed on January 25, 2023. Four (4) New Hampshire residents will be sent letters on January 30, 2023. We have no information that personal information was actually disclosed. However, out of an abundance of caution, we informed individuals whose personal information was contained in the account subject to the incident and provided them with information on how to protect their personal information.

On January 30, 2023, Vice notified the affected New Hampshire residents via the attached sample letter and is offering twelve (12) months of credit monitoring and identity protection services through Equifax to those with Social Security numbers involved. Vice has also taken measures to enhance the security of its network to minimize the likelihood that an event like this might occur again in the future.

Please contact me at lgodfrey@constangy.com should you have any questions.

Sincerely,

Lauren D. Godfrey, CIPP (US/E) of
CONSTANGY, BROOKS, SMITH &
PROPHETE LLP

Encl: Sample Consumer Notification Letter

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

To Enroll, Please Visit
www.equifax.com/activate

Activation Code: **<<code>>**

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

<<Date>>

Re: <<Variable Header>>

Dear <<Name 1>>,

We are writing to inform you of a recent data security incident experienced by Vice Media LLC ("Vice") that may have involved your information. Vice takes the privacy and security of your information very seriously. This communication is being provided to you out of an abundance of caution, as we have no evidence that your personal information has been used inappropriately. Please read this letter carefully as it contains background information about the incident, the type of information involved, and steps you can take to protect your information.

What Happened? On or around March 29, 2022, Vice was alerted to unusual activity within its digital environment. Upon discovering this activity, Vice immediately took steps to secure its network. Vice also engaged leading cybersecurity firms to conduct an investigation to determine what happened and whether personal information hosted on its network may have been involved. The investigation revealed that there may have been unauthorized access to an internal Vice e-mail account. Following a thorough review of the information contained in the email account, we determined that some of your personal information may have been contained within the account. We then worked to obtain up-to-date addresses to notify you of the incident. That process was completed on January 25, 2023. We have no information that your personal information was actually disclosed. However, out of an abundance of caution, we are writing to inform you of the incident and to provide you with information on how to protect your personal information.

What Information Was Involved. The information contained within the email account may have included your name and <<Impacted Data>>.

What We Are Doing. As soon as we were informed of this incident, we took the measures referenced above. As part of the response process, we implemented additional security measures to reduce the risk of a similar incident occurring in the future. Further, we are providing you with notice of this potential incident and steps you can take to protect your personal information. We are also providing you with <<CM Length>> months of identity and credit monitoring services, identity restoration services and up to $1,000,000 identity theft insurance through Equifax.

What You Can Do. You can follow the recommendations included with this letter to help protect your information. Specifically, we recommend that you review your credit report for unusual activity. If you see anything that you do not understand or that looks suspicious, you should contact the consumer reporting agencies for assistance using the contact information included with this letter. In addition, you can enroll in the free identity and credit monitoring services that we are offering to you through Equifax Credit Watch™ Gold. **Enrollment instructions are included with this letter. The deadline to enroll in these services is <<Enrollment Deadline>>.**

For More Information. Further information about how to protect your personal information is included with this letter. If you have any questions regarding the incident, please call between 9:00 am to 9:00 pm Eastern Time from Monday to Friday.

Sincerely,

Vice Media LLC

Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-888-378-4329
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-800-831-5614
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze 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 obtain credit. You must separately place a security freeze on your credit file with 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
riag ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

<FIRST NAME> <LAST NAME>

Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: <<*DEADLINE MMMM DD, YYYY*>>

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 of ***<<ACTIVATION CODE>>*** then click "Submit" and follow these 4 steps:

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.*