



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

RECEIVED

NOV 24 2020

CONSUMER PROTECTION

Amanda N. Harvey
Office: (267) 930-1697
Fax: (267) 930-4771
Email: aharvey@mullen.law

4843 Colleyville Blvd, Suite 251-388
Colleyville, TX 76034

November 19, 2020

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Backroads, located at 801 Cedar Street, Berkeley, CA 94710, and are writing to notify your Office of an incident that may affect the security of some personal information relating to sixteen (16) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Backroads 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.

Nature of the Data Event

On or about October 2, 2020, Backroads became aware of suspicious activity within its computer network. Upon learning of this activity, Backroads immediately began an investigation and worked with third party forensic specialists to determine the nature and scope of the activity. Backroads took steps to secure the network. Through this investigation, Backroads determined that certain files were encrypted and inaccessible. On or about October 16, 2020, Backroads learned that certain files were accessible to unknown actors and removed from Backroads' environment prior to the encryption of Backroads systems.

Once the scope and nature of the suspicious activity were confirmed, Backroads immediately undertook a comprehensive review of the files to identify those whose personal information may have been accessible. This review was completed on October 30, 2020. The investigation confirmed that the following information related to personal information was stored within one of the impacted network devices and may have been accessible to the unknown actor: your name, date of birth, Social Security number, government issued ID, financial account information and health insurance information, if obtained through Backroads. The information was not the same for each individual who was impacted.

Notice to New Hampshire Residents

On or about November 19, 2020, Backroads provided written notice of this incident to affected individuals, which includes sixteen (16) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, Backroads moved quickly to investigate and respond to the incident, assess the security of Backroads email accounts and relevant systems, and notify potentially affected individuals. Backroads is also working to implement additional safeguards and training to its employees.

While Backroads is not aware of any actual or attempted misuse of this information, Backroads is providing access to credit monitoring services for one (1) year, through Epiq, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Backroads is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, 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, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Office of the New Hampshire Attorney General

November 19, 2020

Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1509.

Very truly yours,

A handwritten signature in black ink, appearing to read "Amanda N. Harvey". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Amanda N. Harvey of
MULLEN COUGHLIN LLC

ANH
Enclosure

EXHIBIT A



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

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

RE: Notice of Data Breach

Dear <<Name 1>>,

Backroads writes to inform you of a recent incident that may affect some of your personal information. While we are unaware of any actual or attempted misuse of your information, we want to provide you with information about the incident, our response, and steps you may take to better protect your personal information, should you feel it necessary to do so.

What Happened? On October 2, 2020, Backroads became aware of suspicious activity within its computer network. Backroads immediately began an investigation, working with external forensic specialists, to determine the nature and scope of the activity. Our investigation determined that certain files within our environment were encrypted and inaccessible. On October 16, 2020, we discovered that certain files had been accessible to unknown actors and that certain personal information was contained in these files. We recognize that it may feel like there was a delay between the initial incident and receiving this notification. From the moment we knew that files were accessible to the unknown actors, we have been working both internally to determine who could have been affected, as well as externally with appropriate authorities in each jurisdiction where we operate globally. Thank you for your understanding and patience while we worked through all the necessary details.

What Information Was Involved? Backroads has both legal authority and obligation to maintain personal information for its employees. The forensic investigation confirmed that the following information was stored within one of the impacted network devices and may have been accessible to unknown actors: your name, date of birth, Social Security number, government issued ID (passport or driver's license, if provided to Backroads), financial account information and health insurance information, if obtained through Backroads. While we cannot confirm which piece of your personal information might have been accessed, we are informing employees of the full scope of what could have been compromised due to its presence in impacted files.

What We Are Doing. The confidentiality, privacy, and security of personal information within our custody is among Backroads' highest priorities. In order to minimize the chance that latent malware could remain on Backroads systems, we are rebuilding our network from the ground up, and adding further security measures, to better protect against similar incidents in the future.

What You Can Do. Please review the enclosed *Steps You Can Take to Protect Personal Information*, which contains information on what you can do to better protect against possible misuse of your information.

As an added precaution, Backroads is offering you access to one year of credit monitoring and identity protection services through TransUnion's myTrueIdentity (provided by Epiq) at no cost to you. Details of this offer and instructions on how to enroll in the services are enclosed within this letter.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please call our dedicated hotline at **1-855-914-4688**, Monday through Friday, 6:00 a.m. to 6 p.m. PST, excluding national holidays.

Sincerely,

Tom Hale

Tom Hale
Founder & CEO

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring and Identity Restoration Services

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for one year provided by TransUnion Interactive, a subsidiary of TransUnion*, one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode <<Insert static six-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Monitor Your Accounts

In addition to enrolling in the complimentary services detailed above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements and explanation of benefits, and to monitor your credit reports for suspicious activity and to detect errors. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/freeze/center.html	TransUnion P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 www.transunion.com/credit-freeze	Equifax P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 www.equifax.com/personal/credit-report-services
---	--	---

In order to request a security freeze, you will need to provide the following information:

1. Your 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, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian P.O. Box 9554 Allen, TX 75013 1-888-397-3742 www.experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert	Equifax P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 www.equifax.com/personal/credit-report-services
---	---	--

Additional Information

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.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft. **Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300. **Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023. **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 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 a violator. 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. You can 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. **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/>. **North Carolina Residents:** Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400, 877-566-7226 (toll free within NC). **Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392. **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 5 Rhode Island residents impacted by this incident. **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.