



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

RECEIVED  
JUL 15 2019  
CONSUMER PROTECTION

Jeffrey J. Boogay  
Office: 267-930-4784  
Fax: 267-930-4771  
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

July 9, 2019

**VIA U.S. MAIL**

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

**Re: Notice of Data Security Incident**

Dear Attorney General MacDonald:

We represent Intrepid Benefits Colorado (“Intrepid”) located at 1900 Grant Street, Suite 650, Denver, Colorado 80203 and are writing on behalf of the below entities to notify your office of an incident that may affect the security of some personal information relating to two (2) New Hampshire residents. Intrepid is a third-party benefits administrator for the following entities (collectively referred to as “Clients”) and includes the total number of impacted individuals in parenthesis below:

- CBSR Services Inc. dba Traemand, 750 W Hampden Ave, Suite 250, Englewood, CO 80110, (1)
- Clean Energy Collective, 361 Centennial Pkwy #300, Louisville, CO 80027, (1)

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, Intrepid 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 March 27, 2019, Intrepid discovered suspicious activity related to an Intrepid employee’s email account. Intrepid immediately took steps to secure the employee’s email account by changing the account credentials and launched an investigation. This investigation included working with a third-party forensic investigator to determine the nature and scope of the activity. On April 12, 2019, Intrepid determined that the email account owner was the victim of a phishing attack that

resulted in their account credentials being used by an unknown actor(s) to gain unauthorized access to the employee's email account. Although the investigation confirmed the unauthorized actor(s) gained access between February 19, 2019 and March 26, 2019, Intrepid cannot rule out the possibility of the individual(s) gaining access to any specific email or attachment in the account.

With the assistance of third-party forensics, Intrepid completed a programmatic and manual review of the contents of the email account to determine the types of protected information contained in the emails and to which individuals the information relates, and immediately launched a review of its files to ascertain address information for the impacted individuals. The information that could have been subject to unauthorized access includes name, age or date of birth, hire date, zip code, Social Security number, Plan ID number and Member ID number. On or about May 24, 2019, Intrepid notified each impacted Client of this incident and is providing notice to impacted individuals and regulators, as required, on its Clients' behalf.

#### **Notice to New Hampshire Residents**

On or about July 9, 2019, Intrepid began providing written notice of this incident to all affected individuals, which includes two (2) 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, Intrepid moved quickly to investigate and respond to the incident, assess the security of Intrepid's systems, and notify potentially affected individuals. Intrepid immediately reset the email account password and is also working to implement additional safeguards and training to its employees.

While Intrepid is not aware of any attempted or actual misuse of personal information, Intrepid is providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for two years, through TransUnion, at no cost to these individuals.


Additionally, Intrepid is and will be providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Intrepid is providing individuals with 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.

Attorney General Gordon J. MacDonald  
July 9, 2019  
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) 930-4784.

Very truly yours,

A handwritten signature in blue ink, appearing to read 'JJB', is written over a faint rectangular stamp area.

Jeffrey J. Boogay of  
MULLEN COUGHLIN LLC

JJB/plm  
Enclosure

# **EXHIBIT A**



Return Mail Processing Center  
P.O. Box 9349  
Dublin, OH 43017

<<Name 1>>  
<<Address 1>>  
<<Address 2>>  
<<City>>, <<State>> <<Zip>>  
<<Country>>

July 9, 2019

Dear [NAME]:

Intrepid Benefits, Inc. ("Intrepid") is writing to inform you of a recent event that may impact the security of some of your personal information. Intrepid received your information to assist [Employer – Column A] in the administration of [Employer – Column A]'s health plan. While we are unaware of any actual or attempted misuse of your personal information, we are providing you with information about the incident, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

**What Happened?** On March 27, 2019, Intrepid learned of suspicious activity in an Intrepid employee's email account. We immediately took steps to secure the employee's email account, we immediately took steps to secure the employee's email account and launched an investigation which included working with a leading third-party forensic investigation firm to determine the nature and scope of the activity. On April 12, 2019, Intrepid determined that the email account owner was the victim of a phishing event and an unknown actor had gained access to the Intrepid employee's email account between February 19, 2019 and March 26, 2019. During this limited timeframe, the unauthorized actor may have had access to certain emails and attachments within the account.

**What Information Was Involved?** On April 30, 2019, with the assistance of third-party forensics, Intrepid completed a programmatic and manual review of the contents of the email account to determine the types of protected information contained in the emails and to which individuals the information relates, and immediately launched a review of its files to ascertain address information for the impacted individuals. Our review confirmed that the following types of information were in the email account and may have been accessible to the unauthorized actor: name, date of birth, Social Security number, address, gender, salary, and job title. To date, Intrepid has not received any reports of actual or attempted misuse of your information.

**What We Are Doing.** The confidentiality, privacy, and security of information in our care is one of our highest priorities and we take this incident very seriously. When we discovered this incident, we immediately reset the account password and took steps to determine what personal data was at risk. We also confirmed the security of our employee email accounts and systems. As part of our ongoing commitment to the security of personal information in our care, we are working to review our existing policies and procedures, to implement additional safeguards, and to provide additional training to our employees on data privacy and security. We notified your employer regarding this incident and we also will be notifying state and federal regulators, as required.

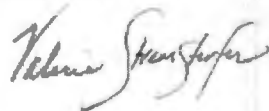
As an added precaution, we are also offering you complimentary access to two years of credit and identity monitoring, fraud consultation and identity theft restoration services through TransUnion. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you. Please review the instructions contained in the attached *Steps You Can Take to Protect Your Information* for additional information on these services.

**What You Can Do.** You may review the enclosed *Steps You Can Take to Protect Your Information*, which contains information on what you can do to better protect against the possibility of identity theft and fraud should you feel it is appropriate to do so. You may also enroll to receive the free credit monitoring and identity theft protection services we are offering.

**For More Information.** We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call Intrepid at our dedicated assistance line at 877-202-8994 Monday through Friday 9am to 9pm ET. You may also write to Intrepid at 1900 Grant Street, Suite 650, Denver, Colorado 80203.

We sincerely regret any inconvenience or concern this incident has caused.

Sincerely,

A handwritten signature in cursive script, appearing to read "Valerie Stremsterfer".

Valerie Stremsterfer  
President  
Intrepid Benefits, Inc.

## **STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION**

### **Enroll in Credit Monitoring**

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for two years provided by TransUnion Interactive, a subsidiary of TransUnion,<sup>®</sup> 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](http://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 697721 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 **October 31, 2019**. 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.

### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH COMPLIMENTARY CREDIT MONITORING SERVICE:**

- Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

### **Monitor Your Accounts**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. 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](http://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**  
PO Box 9554  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**  
P.O. Box 2000  
Chester, PA 19016  
1-888-909-8872

[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

**Equifax**  
PO Box 105788  
Atlanta, GA 30348-5788  
1-800-685-1111

[www.equifax.com/personal/credit-report-services](http://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.);
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 2002  
Allen, TX 75013  
1-888-397-3742

[www.experian.com/fraud/center.html](http://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](http://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](http://www.equifax.com/personal/credit-report-services)

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at [www.irs.gov/Individuals/Identity-Protection](http://www.irs.gov/Individuals/Identity-Protection) for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit [www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft](http://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft) for more 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](http://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 and your state Attorney General. This notice has not been delayed by law enforcement.

**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, [www.ncdoj.gov](http://www.ncdoj.gov).



**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, [www.oag.state.md.us](http://www.oag.state.md.us).

**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 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 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. 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](http://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 Rhode Island Residents:** The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.