



Kamran Salour  
650 Town Center Drive, Suite 1400  
Costa Mesa, CA 92626  
Kamran.Salour@lewisbrisbois.com  
Direct: 714.966.3145

October 18, 2021

File No. 6234.14569

**VIA WEBSITE PORTAL**

Attorney General Gordon MacDonald  
Office of the Attorney General  
Consumer Protection Bureau  
33 Capitol Street  
Concord, NH 03301  
Email: [DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov)

Re: Notification of Data Security Incident

Dear Attorney General MacDonald:

We represent Direct Travel, Inc. ("Direct Travel"), located in Centennial, Colorado, in connection with a data security incident described in greater detail below. Direct Travel takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

**1. Nature of the security incident.**

On April 28, 2021, our cloud-service-provider advised us that it had a data security incident during which some of Direct Travel's data may have been acquired by an unauthorized individual. Our cloud-service-provider retained third-party experts to conduct a forensic investigation to identify, among other things, any Direct Travel documents that may have been impacted. This process took several weeks to perform their review and thereafter, we requested that our cloud-service-provider provide us with those Direct Travel documents. We analyzed those documents to identify those containing the personal information of any Direct Travel customers. The potentially affected information includes dates of birth and/or passport numbers. Direct Travel's investigation determined current address information for the affected individuals in order to effectuate written notification of the incident. This investigation identified four (4) New Hampshire residents within the affected population.

**2. Number of New Hampshire residents affected.**

Direct Travel mailed notification letters to the four (4) New Hampshire residents regarding this data security incident via first-class U.S. mail on October 18, 2021. A sample copy of the notification letter is attached hereto.

**3. Steps taken relating to the incident.**

Direct Travel has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included working with leading cybersecurity experts to enhance the security of its network and increasing its password complexity requirements. Direct Travel is also offering the potentially affected individuals Identity Monitoring services at no cost through Transunion, to ensure their information is protected.

**4. Contact information.**

Direct Travel remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (714) 966-3145 or via email at Kamran.Salour@lewisbrisbois.com.

Regards,

/s/ Kamran Salour

Kamran Salour of  
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure(s): Consumer Notification Letter



# Direct Travel

Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

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

To enroll, please call:  
**1-855-288-5422**  
or visit:  
**www.MyTrueIdentity.com**  
Enrollment Code: <<Activation Code>>  
Pass Code: <<Pass Code>>

<<Date>>

Re: Notice of Data Security Incident

Dear <<Name 1>>,

We at Direct Travel, Inc. take the privacy and security of your information seriously. That is why we write to inform you of an incident impacting our cloud-service-provider that may have involved some of your personal information. This letter describes the incident, identifies the information that the incident involved, states the steps that we have taken in response to the incident, and advises you of certain steps that you can take to help protect your personal information, including activating the credit and identity monitoring services that we are offering at no cost to you.

**What Happened?** On April 28, 2021, our cloud-service-provider advised us that it had a data security incident during which some of Direct Travel’s data may have been acquired by an unauthorized individual. Our cloud-service-provider retained third-party experts to conduct a forensic investigation to identify, among other things, any Direct Travel documents that may have been impacted. This process took several weeks to perform their review and thereafter, we requested that our cloud-service-provider provide us with those Direct Travel documents. We analyzed those documents to identify those containing the personal information of any Direct Travel customers. Although we have no evidence to suggest that any of your information has been misused, we are notifying you of this incident out of an abundance of caution.

**What Information Was Involved?** The files that the unauthorized actor may have accessed contain customer personal information including dates of birth and/or passport numbers.

**What Are We Doing?** As soon as we learned of the incident, we took the steps described above. In addition, we have secured the services of Transunion to provide identity monitoring at no cost to you for 12 months. Transunion 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. Those services are described in further detail below.

To receive these services, you must be over the age of 18, 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. Additional information describing your services is included with this letter.

Please note you must enroll by <<Enrollment Deadline>>. If you have questions or need assistance, please visit [www.MyTrueIdentity.com](http://www.MyTrueIdentity.com) or call 1-855-288-5422.

**What You Can Do:** Please review the enclosed “Additional Resources” section included with this letter. It describes additional steps you can take to help safeguard your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file. We also encourage you to activate the complimentary identity monitoring services we are making available through Transunion.

Direct Travel, Inc.  
7430 E. Caley Avenue, Suite 320E  
Centennial, CO 80111

**For More Information:** If you have questions or need assistance, please call 855-675-2844, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, except holidays.

Protecting your information is important to us. Please know that we take this incident very seriously, and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read "John Coffman", is displayed on a light blue rectangular background.

John Coffman  
Chief Financial Officer  
Direct Travel, Inc.

## Additional Resources

**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 incidence 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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact one of the following three national credit reporting agencies:

**TransUnion**

P.O. Box 1000  
Chester, PA 19016  
1-800-909-8872

[www.transunion.com](http://www.transunion.com)

**Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742

[www.experian.com](http://www.experian.com)

**Equifax**

P.O. Box 105851  
Atlanta, GA 30348  
1-800-685-1111

[www.equifax.com](http://www.equifax.com)

**Free Annual Report**

P.O. Box 105281  
Atlanta, GA 30348  
1-877-322-8228

[www.annualcreditreport.com](http://www.annualcreditreport.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 90 days. 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:** Under U.S. law, 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. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, [www.consumer.ftc.gov](http://www.consumer.ftc.gov) and [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), 1-877-438-4338. Residents of New York, Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

**New York Attorney General**

**Bureau of Internet and  
Technology Resources**

28 Liberty Street  
New York, NY 10005  
[ifraud@ag.ny.gov](mailto:ifraud@ag.ny.gov)  
1-212-416-8433

**Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[www.oag.state.md.us](http://www.oag.state.md.us)  
1-888-743-0023

**North Carolina Attorney  
General**

9001 Mail Service Center  
Raleigh, NC 27699  
[www.ncdoj.gov](http://www.ncdoj.gov)  
1-877-566-7226

**Rhode Island**

**Attorney General**

150 South Main Street  
Providence, RI 02903  
[www.riag.ri.gov](http://www.riag.ri.gov)  
401-274-4400

**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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit [http://files.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf).



Activation Code: <<Activation Code>>

**1-Bureau TransUnion Credit Monitoring Product Offering:** (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for 12 months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at [www.mytrueidentity.com](http://www.mytrueidentity.com) and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<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 following 6-digit telephone pass code <<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.

Once you are enrolled, you will be able to obtain 12 months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. 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, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online 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 credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.