LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Christopher E. Ballod
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Christopher.Ballod@lewisbrisbois.com
Direct: 215.977.4077

January 24, 2020

VIA E-MAIL
Gordon MacDonald, Attorney General
Consumer Protection and Antitrust Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent Travel Tripper, LLC ("Travel Tripper"), a hotel technology provider based in New York, New York. This letter is being sent pursuant to N.H. Rev. Stat. §§ 359-C:19-21, because the personal information of New Hampshire residents may have been affected by a recent data security incident. The incident may have included unauthorized access to names, billing addresses, and credit card numbers for certain hotel customers who used credit cards to reserve rooms between approximately October 15 and October 22, 2019.

In October of 2019, Travel Tripper discovered unusual activity in its Central Reservation System – a computerized reservation software used to maintain hotel information, room inventory and rates, and to manage the reservation process. While consumer credit card information is tokenized and subsequently processed by a hotel's property management system, the Central Reservation System stores cardholder data for future use by the hotel properties, as needed. Upon discovering this unusual activity, Travel Tripper immediately took steps to secure its system and launched an investigation with the assistance of an external digital forensics firm to help determine what occurred and whether sensitive information was accessed or acquired without authorization as a result. Travel Tripper also reported the incident to law enforcement. On December 9, 2019, the forensics firm reported that an unauthorized actor may have accessed or acquired payment card information for certain reservations contained within the Central Reservation System by legitimately accessing the portal with compromised credentials. On January 17, 2020, Travel Tripper identified two (2) New Hampshire residents included within the potentially affected population.

Travel Tripper is not aware of any unauthorized credit card transactions or fraudulent activity as a result of this incident. Travel Tripper has notified its impacted hotel property customers and is notifying affected consumers on the hotel properties' behalf. In response, Travel Tripper has implemented enhanced security measures to minimize the likelihood that an event like this might occur again in the future. Travel Tripper notified the affected New Hampshire residents via the attached sample letter on January 24, 2020. Out of an abundance of caution, Travel Tripper is offering twelve (12) months of complimentary credit and identity monitoring services to the affected residents through ID Experts.

Please contact me should you have any questions.

Sincerely,

Christopher E. Ballod of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

travel tripper

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR, 97223

To Enroll, Please Call:
1-833-719-0133
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
[XXXXXXXX]

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

January XX, 2020

Re: Notice of Security Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of a data security incident experienced by Travel Tripper that may have involved some of your personal information. We are also writing you to recommend immediate action that you can follow to help protect your personal information. Travel Tripper provides online reservation booking services for numerous hotels, including a hotel property where you recently booked a reservation. As explained below, we discovered that there may have been unauthorized access to a Travel Tripper account containing your name, address, and credit card information that you provided in connection with an online reservation you made at one of those properties. In an abundance of caution, we wanted to notify you of the incident, offer you identity protection services, and inform you about steps that can be taken to help protect your personal information.

What Happened? On October 23, 2019, we learned that cardholder data accessible to a Travel Tripper user account may have been accessed or acquired without authorization. Upon discovering this, we immediately took steps to secure the system and launched an investigation. We also engaged a leading digital forensics firm to determine what happened and whether sensitive information was accessed or acquired without authorization as a result. On December 9, 2019, our investigation determined that your credit card information may have been accessed without authorization at some time during the period from October 15 to October 22, 2019. Travel Tripper is not currently aware of any unauthorized credit card transactions or fraudulent activity having occurred as a result of this incident. We are notifying you now out of an abundance of caution.

What Information Was Involved? The information involved may have included names, addresses, and credit card numbers with card security codes and expiration dates.

What We Are Doing. As soon as we discovered this incident, we took the measures referenced above and implemented enhanced security measures in order to better safeguard all sensitive data in our possession and to help prevent a similar incident from occurring in the future. We also reported the matter to law enforcement and will provide whatever cooperation is necessary to hold the perpetrator accountable. In addition, we are providing you information about steps you can take to protect your personal information and identity theft protection services through ID Experts®, a data security and recovery services expert. Your complimentary one-year enrollment in MyIDCare™ includes: credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. Additional information about these services is included with this letter.

What You Can Do. Please read the recommendations included with this letter which you can follow to help protect your personal information. You can also enroll in the MyIDCare services being provided to you, at no cost, through ID Experts. To enroll, please visit the MyIDCare website at **https://app.myidcare.com/accountcreation/protect** and provide your enrollment code located at the top of this page. Please note that you should enroll as soon as possible, but the deadline to enroll is April XX, 2020. Additional information describing the MyIDCare services, along with other recommendations to protect your personal information, is included with this letter.

For More Information. Please accept our sincere apologies for any worry or inconvenience that this may cause you. If you have any questions about the incident or how to enroll in the complimentary services that we are offering, please call 1-833-719-0133 Monday through Friday from 9 am to 9 pm Eastern Time, or please visit the MyIDCare website at **https://app.myidcare.com/accountcreation/protect** for assistance or for any additional questions you may have. Please have your enrollment code ready.

Sincerely,

Joan Lee
Vice President of Operations
Travel Tripper, LLC
370 Lexington Ave, Suite 1601
New York, NY 10017

Steps You Can Take to Further Protect Your 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 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	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-877-322-8228	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	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: You have the right to put a security freeze on your credit file. 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. There is no charge to place, lift or remove the security freeze. 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 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. Residents of Maryland, North Carolina, and Rhode Island can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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.

MyIDCare™

One-Year Enrollment in MyIDCare™

Website and Enrollment. Please visit **https://app.myidcare.com/account-creation/protect** and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

Telephone. Contact MyIDCare at 1-833-719-0133 or to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

This MyIDCare enrollment will include one-year enrollment into:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCAN™ - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to $1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY - ID Experts' fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned IDCare Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.