Baker McKenzie.

STATE OF NH
DEPT. OF JUSTICE
2018 SEP 24 P 2:49

Baker & McKenzie LLP

452 Fifth Avenue
New York, NY 10018
United States

Tel: +1 212 626 4100
Fax: +1 212 310 1600
www.bakermckenzie.com

Asia Pacific
Bangkok
Beijing
Brisbane
Hanoi
Ho Chi Minh City
Hong Kong
Jakarta
Kuala Lumpur*
Manila*
Melbourne
Seoul
Shanghai
Singapore
Sydney
Taipei
Tokyo
Yangon

Europe, Middle East & Africa
Abu Dhabi
Almaty
Amsterdam
Antwerp
Bahrain
Baku
Barcelona
Berlin
Brussels
Budapest
Cairo
Casablanca
Doha
Dubai
Dusseldorf
Frankfurt/Main
Geneva
Istanbul
Jeddah*
Johannesburg
Kyiv
London
Luxembourg
Madrid
Milan
Moscow
Munich
Paris
Prague
Riyadh*
Rome
St. Petersburg
Stockholm
Vienna
Warsaw
Zurich

The Americas
Bogota
Brasilia**
Buenos Aires
Caracas
Chicago
Dallas
Guadalajara
Houston
Juarez
Lima
Los Angeles
Mexico City
Miami
Monterrey
New York
Palo Alto
Porto Alegre**
Rio de Janeiro**
San Francisco
Santiago
Sao Paulo**
Tijuana
Toronto
Valencia
Washington, DC

* Associated Firm
** In cooperation with Trench, Rossi e Watanabe Advogados

September 20, 2018

Via certified mail

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Dear Attorney General,

I write on behalf of Protravel International LLC ("**Protravel**") to notify you that a handful of Protravel travel agents were the target of a phishing attack that resulted in the compromise of certain customer information. The intrusion was discovered by Protravel on approximately August 22, 2018.

Specifically, Protravel learned that between approximately October 25, 2017 and April 25, 2018, a limited number of travel agents affiliated with Protravel became victims of a phishing incident that allowed unauthorized access to the agents' email accounts and customer communications. As soon as Protravel identified the intrusion, they took prompt action to halt it. Protravel estimates that approximately **1** resident of your State was affected by this incident.

For the limited number of customers who provided personal information in the body or attachment to an email they sent to one of the affected agents, the intruder may have gained access to travel-related information, including passport or driver's license number, and certain payment card or bank account information.

Following the discovery of this intrusion, Protravel also retained independent cyber forensic consultants to investigate the root cause of the intrusion, identify those affected, and put in a place a remediation plan to prevent recurrence. Protravel is in the process of implementing multi-factor authentication for travel agents with access to its systems. Additionally, Protravel agents will be provided with phishing and general data protection training.

Protravel will provide postal mail notifications to impacted customers, informing them about the incident, and encouraging them to take security precautions regarding their personal information. Protravel is also offering credit protection services at no cost to the impacted individuals. Protravel has also encouraged potentially affected consumers to be vigilant of email, telephone, and other potential scams asking for any personal information.

Affected individuals may contact Protravel's dedicated hotline established for this matter at 866-775-4209 to clarify or address any questions or concerns. We attach a copy of the sample customer notice. Please feel free to contact me directly at **(212) 626-4285** or harry.valetk@bakermckenzie.com.

Sincerely,

Harry A. Valetk

Baker & McKenzie LLP is a member of Baker & McKenzie International.

PROTRAVEL
INTERNATIONAL

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>
<<ClientDef1 (CareOfHeadofHousehold)>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Re: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

We write to notify you about a data security incident that may have inadvertently exposed some of your personal information. We take the protection and proper use of your information very seriously, and contact you now to explain what happened and the steps you can take to protect yourself against identity fraud.

What happened?

Between approximately October 25, 2017 and April 25, 2018, a limited number of travel agents affiliated with Protravel International, LLC (**"Protravel"**) became victims of a phishing incident that allowed an unauthorized person to gain access to the agents' email accounts and customer communications. Based on our investigation, some of your personal information may have been included in the body of an email or as an attachment within an affected agent's account. As soon as Protravel identified the situation, we took immediate action to halt it, and have been continuously working with external cyber forensic consultants to determine both the cause and the scope of the data incident.

What information was involved?

The types of personal information exposed vary depending on what travel-related details were sent by email, but may include your passport or driver's license number, or your payment card number or bank account number, but only to the extent you, or someone on your behalf, provided this information to your travel agent by email. At this point, we have no evidence that any of your personal information was used to commit identity fraud.

What are we doing?

We have been working with external cyber forensic consultants to help us investigate the impacted agent communications, and we are taking important steps to prevent a similar event from reoccurring. Additionally, we are taking steps to provide additional education to our affiliated travel agents regarding suspected phishing emails, and to enhance our monitoring for, and prevention of, these types of incidents.

To help relieve concerns and restore confidence following this incident, we have also secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll 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.

Visit **<<IDMonitoringURL>>** to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

For Adults Only

Your identity monitoring services include Credit Monitoring, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

To receive credit services by mail instead of online, please call 1-???-???-????. Additional information describing your services is included with this letter.

For Minors Only

Your identity monitoring services include Minor Identity Monitoring, Fraud Consultation, and Identity Theft Restoration.

Minor Identity Monitoring instructions.

Visit **<<IDMonitoringURL>>** to activate and take advantage of Minor Identity Monitoring.

After you have logged in for the first time, you will see a screen with the title "Confirm Your Information". Before Minor Identity Monitoring services can be activated, you must follow the instructions below:

1. Change the "First Name" and "Last Name" fields to a parent or guardian's name.
2. Change the address that appears to the parent or guardian's current address.
3. Enter the parent or guardian's date of birth and Social Security number.
4. Enter the email address and password you would like to use for the account. Choose a security question and enter the security answer.
5. Click the "Create Account" button. After the account is created, you will be able to activate your child's Identity monitoring service.

Additional information describing your services is included with this letter.

What can you do?

We encourage you to be especially aware of email, telephone, and postal mail scams that ask for personal or sensitive information. In addition, if you have any pending travel-related transactions, use extra caution and diligence in any online communications. It is important to always verbally verify over the telephone with your agent about any wiring instructions you may receive about your itinerary. Use phone numbers that you know to be correct rather than phone numbers included in an email. Be suspicious of emails that communicate updated, revised, or corrected wiring or payment instructions.

Please note that although Protravel is offering to provide identity monitoring services for one year free of charge via Kroll, the consumer reporting agencies listed below may charge fees for their services.

Again, we take the privacy and security of your information seriously, and sincerely regret any concern or inconvenience that this incident may have caused you. If you have questions, please call 1-???-???-????, Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time.

Sincerely,

Michele Capaccio
Senior Vice President, Operations

Other Important Information

To protect against possible identity fraud or other financial loss, we encourage you to remain vigilant, review your financial account statements, and monitor your credit reports. Protravel is also providing the following information for those who wish to consider it:

- For more information about how to protect yourself from identity theft, visit the website of the U.S. Federal Trade Commission (**"FTC"**) at http://www.consumer.ftc.gov/features/feature-0014-identity-theft or reach the FTC at 877-382-4357 or 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, and the FTC.
  - **North Carolina Residents.** You can reach the North Carolina Attorney General directly at 919-716-6400 or Office of the Attorney General, 9001 Mail Service Center, Raleigh, North Carolina 27699
- You may have the right to obtain any police report filed related to this intrusion, and to file a police report and obtain a copy of it if you are the victim of identity theft.
- Under U.S. law, U.S. residents are entitled to one free credit report annually from each of the three major credit bureaus. To order your free credit report, visit www.annualcreditreport.com or call toll-free 877-322-8228.
- You can request information regarding "fraud alerts" and "security freezes" from the three major U.S. credit bureaus listed below. At no charge, if you are a U.S. resident, you can have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. While this service can effectively make it more difficult for someone to get new credit in your name, it may also delay your own ability to obtain credit while the agency verifies your identity. A "security freeze" generally prohibits the credit reporting agency from releasing your credit report or any information from it without your written authorization. You should be aware that placing a security freeze on your own credit profile may delay or interfere with the timely approval of any new requests that you make for loans, credit, mortgages, or other debt services. Unlike fraud alerts, to obtain a security freeze you must send a written request to each of the three major reporting agencies and you may be required to provide information such as your: (1) name; (2) Social Security number; (3) date of birth; (4) current address; (5) addresses over the past five years; (6) proof of current address; (7) copy of government identification; and (8) any police/investigative report or complaint. If you wish to place a fraud alert or a security freeze, or if you have any questions about your credit report, please contact any one of the consumer reporting agencies listed below:
  - **Experian:** 888-397-3742; www.experian.com; P.O. Box 9554, Allen, TX 75013
  - **Equifax:** 800-525-6285; www.equifax.com; P.O. Box 105788, Atlanta, GA 30348
  - **TransUnion:** 800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022-2000

Kroll.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

For Adults Only

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

For Minors Only

Minor Identity Monitoring

Minor Identity Monitoring detects when names, addresses, and credit information is associated with your child's Social Security number. An alert will be sent when activity is detected. The presence of a credit file may be an indicator of identity theft or fraud for children who, as minors, should not have a credit history.

For Adults and Minors

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

1 Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and 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.