

**KELLEY DRYE & WARREN LLP**

A LIMITED LIABILITY PARTNERSHIP

WASHINGTON HARBOUR, SUITE 400

3050 K STREET, NW

WASHINGTON, D.C. 20007-5108

(202) 342-8400

FACSIMILE

(202) 342-8451

www.kelleydrye.com

ALYSA Z. HUTNIK

DIRECT LINE: (202) 342-8603

NEW YORK, NY

LOS ANGELES, CA

CHICAGO, IL

STAMFORD, CT

PARSIPPANY, NJ

BRUSSELS, BELGIUM

AFFILIATE OFFICE

MUMBAI, INDIA

September 22, 2014

**VIA OVERNIGHT DELIVERY**

Office of the Attorney General  
State of New Hampshire  
Attn: Security Breach Notification  
33 Capitol Street  
Concord, NH 03301

To Whom It May Concern:

Pursuant to your state's law, Viator is notifying your office of a data compromise that could potentially affect payment card data of approximately 1,556 New Hampshire residents. On September 2, 2014, we were informed by our credit card service provider that unauthorized charges had been made on a number of our customers' credit cards. Although our investigation is continuing, we currently believe that some forms of data may be affected by the compromise. This information includes encrypted credit or debit card number, along with card expiration date, name, billing address, email address, and, if the customer has created a Viator account, the associated email address, encrypted password, and Viator "nickname." Fortunately, we have no reason to believe at this time that the three or four digit value printed on the back or front of the card was compromised. Additionally, Viator does not collect debit PIN numbers.

Viator is dedicating all the resources necessary to investigate and resolve this incident. The company has hired forensic experts, notified law enforcement, and has been working diligently and comprehensively to investigate the incident, identify how its systems may have been impacted, and secure its systems. In addition, Viator is continuously working to strengthen its security measures to help minimize the potential for incidents of this nature in the future. Viator is providing direct notification to customers that may have been affected. Additionally, the company is establishing a dedicated toll-free helpline for further customer information and assistance and offering free identity protection services, including credit monitoring, to its U.S. customers.

Accordingly, please find enclosed a copy of the electronic notice of the data compromise sent to New Hampshire residents on September 19, 2014.

September 22, 2014

Page Two

Please contact us with any questions or concerns.

Sincerely,

A handwritten signature in black ink that reads "Alysa Z. Hutnik". The signature is written in a cursive, slightly slanted style.

Alysa Z. Hutnik

Enclosure

September 19, 2014

**Subject: Important Notice: Data compromise at Viator**

Dear Viator Customer

We want to make you aware that Viator has experienced a data compromise that could potentially affect payment card data used to make bookings through Viator's websites and mobile offerings. If you have created a Viator account, this compromise may also affect your email address, password and Viator "nickname." We deeply regret any inconvenience this may cause. The protection of our customers' personal information is of paramount concern. We are dedicating all the resources necessary to investigate and resolve this incident.

We have alerted the credit card companies and law enforcement, in addition to taking appropriate steps to secure our systems. We are writing to make you aware of the occurrence so that you can also monitor your accounts as a prudent measure, and take any other precautions you believe may be appropriate. We are offering our customers in the U.S. free identity protection services, including credit monitoring.

Meanwhile, we are continuously working to strengthen our security measures to help minimize the potential for incidents of this nature in the future. While our investigation is ongoing, here is some important information to be aware of.

**What Happened:**

On September 2, we were informed by our credit card service provider that unauthorized charges had been made on a number of our customers' credit cards. We have hired forensic experts, notified law enforcement and we have been working diligently and comprehensively to investigate the incident, identify how our systems may have been impacted, and secure our systems. Although our investigation is continuing, we currently believe that some forms of your data may be affected by the compromise. This information includes encrypted credit or debit card number, along with card expiration date, name, billing address, email address and, if you have created a Viator account, the associated email address, encrypted password and Viator "nickname." At this time, we have no reason to believe that the three or four digit value printed at the back or front of your card was compromised. Additionally, debit PIN numbers are not collected by Viator and could therefore not be compromised.

**Steps You Can Take To Further Reduce Your Risk of Identity Theft/Fraud:**

We recommend that all affected customers monitor their card activity and report any fraudulent charges to their credit card company. It is always a good practice to review your credit and debit card account statements regularly for suspicious activity. If you notice suspicious activity involving your account, please report it immediately to the appropriate financial institution or credit card company. You will not be responsible for fraudulent charges to your account if you report them in a timely manner.

To assist our customers in the U.S., we are offering free identity protection services, including credit monitoring. More information on that offer is below.

Additionally, we encourage you to reset your Viator password the next time you sign in to your Viator account, and change it on any other sites where you used the same password.

To change passwords on the Viator site, click on the "Change Password" on the "My Profile" tab, once signed in. Here are some tips to help you create a strong password: (1) make sure your password is at least six characters in length; (2) combine numbers and letters and don't include commonly used words; (3) include punctuation marks; and (4) mix capital and lowercase letters. It is also advisable to use a different password on different sites.

If you have questions related to this situation, you can contact us anytime through our dedicated toll-free information helpline at 888-680-0710 or at 702-939-9819.<sup>1</sup>

Responding properly to this incident is our top priority, and we are committed to taking all appropriate steps to safeguard your personal information. For over 10 years, Viator's mission has been dedicated to offering travelers the best tours and activities worldwide, and to delivering a superior experience in all our customer interactions. That mission continues. We deeply regret any inconvenience or concern this may cause you and we thank you for your patience as we continue our investigation. We are focused on doing everything possible to maintain your trust so that we can continue to serve you in the future.

Sincerely,

Barrie Seidenberg  
CEO, Viator

---

<sup>1</sup> Please do not reply to this email with any personal information.

## Steps You Can Take To Further Protect Your Information

### Review Your Account Statements

As a precautionary measure, we recommend that you review 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, or the Federal Trade Commission. In some states, you may also obtain a police report regarding this incident.

### Free Credit Monitoring

To help protect your identity, we are offering a **complimentary** one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

### Activate ProtectMyID Now in Three Easy Steps

1. ENSURE That You Enroll By: **December 31, 2014** (Your code will not work after this date.)
2. Visit the **ProtectMyID Web Site to enroll: [www.protectmyid.com/redeem](http://www.protectmyid.com/redeem)**
3. PROVIDE Your Activation Code: [code]

If you have questions or need an alternative to enrolling online, please call 866-926-9801 and provide engagement #: [XXXXX].

### Additional details regarding your 12-month ProtectMyID Membership:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.
- **\$1 Million Identity Theft Insurance<sup>2</sup>:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

---

<sup>2</sup> Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of AIG. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 866-926-9801.

### Credit Report Monitoring

You may obtain a free copy of your credit report from each of the 3 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 a copy of the request form at <http://www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf>. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies shown below.

Equifax (800) 685-1111 <a href="http://www.equifax.com">www.equifax.com</a> P.O. Box 740241 Atlanta, GA 30374	Experian (888) 397-3742 <a href="http://www.experian.com">www.experian.com</a> 535 Anton Blvd., Suite 100 Costa Mesa, CA 92626	TransUnion (800) 916-8800 <a href="http://www.transunion.com">www.transunion.com</a> P.O. Box 6790 Fullerton, CA 92834
---	--	--

### Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338). **Maryland residents** may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <http://www.oag.state.md.us/idtheft>, or by sending an email to [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us), or calling 410-576-6491. **North Carolina residents** may wish to review information provided by the North Carolina Attorney General at <http://www.ncdoj.gov>, by calling 877-566-7226, or writing to 9001 Mail Service Center, Raleigh, North Carolina 27699.

### Fraud Alert

You may consider placing a fraud alert on your credit report. This fraud alert statement 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

In some U.S. states, 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. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to \$10 to place, lift, or remove the security freeze; however, this fee may be less in certain states (in MA, up to \$5). 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. You must separately place a security freeze on your credit file with each credit reporting agency.