



January 26th, 2017

BY FIRST-CLASS MAIL

Office of the Attorney General
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

Consistent with N.H. Rev. Stat. 359-C:20(1)(b), this letter provides formal notice of a computer data security incident affecting the RBC travel rewards redemption platform operated by Travelocity (the “Platform”) that we currently estimate affected one individual who resides in New Hampshire.

RBC makes the Platform available to its customers to redeem credit card rewards points for travel reservations. Information submitted by customers on the Platform is maintained by Travelocity on RBC’s behalf. The Platform is entirely separate from RBC’s own network and systems. RBC’s systems are not impacted by this situation in any way and the data on RBC’s systems remains secure.

After an investigation into increased fraudulent activity on RBC-issued payment cards, RBC notified Travelocity that it had observed increased fraudulent payment card activity on RBC-issued cards that were processed on the Platform. Travelocity undertook an investigation with the help of outside cybersecurity experts and, on January 5, notified RBC that there had been unauthorized access to the Platform resulting in the likely exposure of payment card information for cards used on the Platform between October 3, 2017 and December 22, 2017. Specifically, Travelocity’s investigation to date indicates that there likely was unauthorized access to payment card number and CVV (the three- or four-digit security code on the back of the credit card). While other personal information is submitted on the Platform, the Travelocity investigation to date has not found any evidence of unauthorized access to this information. Bank account information and Social Security numbers are not stored on the Platform and were not accessed.

Travelocity has taken a number of steps to contain and remediate this incident by blocking attacker access to the affected environment and remediating impacted systems and accounts. It also implemented additional measures to enhance the general security of this environment, including improving its visibility of potentially unauthorized activity within the environment. It has also notified law enforcement in support of its investigation regarding this incident.

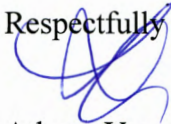
We currently estimate that this incident affected one individual who resides in New Hampshire and whose information was submitted on the Platform between October 3, 2017 and December 22, 2017.

On January 26, 2018, RBC and Travelocity began notifying individuals whose personal information may have been exposed. By January 31, 2018, RBC and Travelocity expect to have notified the one impacted resident of New Hampshire by mail. A sample notification letter to affected individuals is included as Appendix A to this letter.

For affected RBC customers that used an RBC-issued payment card, RBC offers zero-liability coverage for all fraudulent transactions, and has implemented enhanced fraud monitoring. Additionally, RBC offers its customer's access to a TransUnion CreditView Dashboard, which permits customers to view their credit score and credit score history. For affected individuals who are not RBC customers, Travelocity will offer twelve (12) months of complimentary credit monitoring. Additionally, Travelocity have established a call center to provide updated information to affected individuals.

RBC is committed to answering any questions that consumers in your state and members of your office may have. Please feel free to contact me with any questions at 416-974-6655.

Respectfully yours,



Athena Varmazis
Senior Vice President, Credit Cards
RBC Royal Bank

Enclosures

2018 JAN 31 AM 9:41
STATE OF NH
DEPT OF JUSTICE



<Customer Address>

January 26, 2018

Notice of Data Breach Involving RBC Travel Rewards Website Provided by the Travelocity Partner Network (“Travelocity”)

Dear <Name>,

We are writing to tell you about a data security incident involving an RBC vendor. Travelocity operates the travel rewards platform which is used to process RBC's travel rewards redemptions. On January 5, Travelocity notified RBC that there had been unauthorized access to their travel platform resulting in the exposure of payment card information of a limited number of individuals. This incident potentially affects payment card information used to book travel using the RBC Travel Rewards website between October 3, 2017 and December 22, 2017.

Please note that this incident does not involve RBC's own systems.

The enclosed letter from Travelocity details information about the incident and resources that are being offered to protect you.

Since RBC first discovered fraudulent activity related to the travel rewards platform, we have been working closely with the Travelocity team to identify the root cause of the unauthorized access and to enhance the protection of your information. We also immediately put into place enhanced credit card monitoring on your account so you would not be affected by this incident any further.

Safeguarding the security of your information is of the utmost importance to us. Please be assured that you are protected by RBC's Zero Liability Guarantee so you will not be held liable for any unauthorized transactions on your RBC credit card resulting from this incident.

We also encourage you to regularly monitor your accounts and contact us immediately should you notice any unusual or unauthorized activity. As an Online Banking client, you can also monitor your credit reports using our free CreditView Dashboard, which helps you check your credit score regularly with no negative impacts.

If you have questions, please call 1-888-565-0085. We regret any inconvenience you may have experienced as a result of this incident. We remain committed to your security, and greatly appreciate the relationship you have with RBC.

Sincerely,

Athena Varmazis
Senior Vice President, Credit Cards
RBC Royal Bank

Enclosure



January 26, 2018

[NOTICE OF DATA BREACH]

We are writing to make you aware that your payment card information may have been exposed as a result of a data security incident affecting the RBC travel rewards redemption platform operated by Travelocity (the "Platform").

What Happened?

RBC notified Travelocity that it had observed increased fraudulent payment card activity on RBC-issued cards that were processed on the Platform. Travelocity immediately investigated and, on January 5, notified RBC that there had been unauthorized access to the Platform resulting in the likely exposure of payment card information for cards used on the Platform between October 3, 2017 and December 22, 2017.

What Information Was Involved?

The investigation indicates that there likely was unauthorized access to your payment card number and CVV (the three- or four-digit security code on the back of the credit card).

What Information Was *Not* Involved?

While other personal information is submitted on the Platform, the Travelocity investigation to date has not found any evidence of unauthorized access to this information. We can assure you that bank account information and Social Security numbers are not stored on this Platform and were not accessed. Furthermore, this incident only impacted this specific travel rewards partner Platform and we have not identified any impact from this incident on any other Travelocity websites or services.

What We Are Doing

We do and will continue to treat the security of all personal information as a top priority. We took immediate steps to investigate the incident using a leading cybersecurity firm, notified law enforcement and payment card partners about the incident, and enhanced security and monitoring of the affected Platform.

RBC also immediately put into place enhanced credit card monitoring to help ensure you would not be affected by this incident further. You are also protected by RBC's Zero Liability Guarantee so you will not be held liable for any unauthorized transactions on your RBC credit card that result from this incident.

What You Can Do

In addition to the services mentioned above, we recommend that you remain vigilant in regularly reviewing and monitoring your account statements and credit history. If you are an Online Banking client with RBC, you can use their free CreditView Dashboard tool to monitor your credit reports with no negative impact to your credit score.

If you suspect that your payment card has been misused, please contact your financial institution [or call the number on the back of your card]. For RBC-issued payment cards, please contact RBC at 1-888-565-0085. **Attachment A** contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information

If you have any additional questions or concerns about this incident, please call 1-800-204-4048 between the hours of 8:00AM to 6:00PM Eastern time.

We sincerely regret that this occurred, and we apologize for any inconvenience that may have been caused by this incident.

Sincerely,

Daniel Hest
Senior Vice President

Attachment

ATTACHMENT A

Additional Information

To protect against possible fraud, identity theft or financial loss, we encourage you to remain vigilant, review your account statements, and monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit reporting agencies and additional information about steps you can take to obtain a free credit report and to place a fraud alert, credit freeze, or credit lock on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your State's attorney general, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit reporting agencies. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three credit reporting agencies below:

| | | |
|--|--|--|
| Equifax: | Experian: | TransUnion: |
| Consumer Fraud Division | Credit Fraud Center | TransUnion LLC |
| P.O. Box 740256 | P.O. Box 9554 | P.O. Box 2000 |
| Atlanta, GA 30374 | Allen, TX 75013 | Chester, PA 19022-2000 |
| 1-888-766-0008 | 1-888-397-3742 | 1-800-680-7289 |
| www.equifax.com | www.experian.com | www.transunion.com |

Fraud Alert: Consider contacting the three major credit reporting agencies at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the

timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services.

To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

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, 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, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft; and
8. If you are not a victim of identity theft, payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years. The cost to place a credit freeze is typically between \$5.00 and \$10.00 each time you place a freeze, but may vary by jurisdiction. Certain jurisdictions may also permit a credit reporting agency to charge you similar fees to lift or remove the freeze. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a credit freeze.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

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, or the FTC.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file a police report by contacting local or state law enforcement agencies.