

February 20, 2025

VIA E-MAIL

Office of the Maryland Attorney General
Saint Paul Plaza
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Security Incident

To Whom It May Concern:

We represent Towne Vacations Deep Creek, LLC, t/a Railey Vacations (hereinafter, "Railey Vacations"), located at 5 Vacation Way, McHenry, MD 21541. We are writing to notify your office of a recent security incident that may involve two hundred eighty-nine (289) Maryland residents.

1. Background Information and Description of Incident

Railey Vacations is a vacation rental company that assists private homeowners with renting their properties to guests visiting Deep Creek Lake in Maryland.

On October 11, 2024, Railey Vacations became aware of suspicious activity involving an employee's email account. Railey Vacations promptly launched an investigation with the assistance of third-party cybersecurity specialists to understand the nature and extent of this matter. The investigation revealed that an unauthorized person gained access to the employee's email account and the emails within it. Railey Vacations then conducted a review of these emails to determine what personal information was involved and to whom that information belonged.

2. Potentially Involved Information

Although it varies by individual, the following types of information were involved in this incident: Social Security number, driver's license or government ID, passport number, financial account number and routing number, clinical or treatment information, and patient account number. Railey Vacations is not aware of any evidence of fraud or misuse of the involved information.

3. Notifications to Potentially Affected Individuals

On February 20, 2025, Railey Vacations began notifying potentially affected individuals via mailed letter. That letter provides individuals with information and resources to help protect their information. Railey Vacations is also offering 24 months of complimentary identity protection services through Equifax Complete™ Premier to notified individuals, and a call center is currently open and available to address any inquiries related to this matter.

Attached as **Exhibit A** is sample of the consumer notification letter for your reference.

4. Steps Taken in Response to the Incident

In response to this incident, Railey Vacations took steps to prevent a similar incident from reoccurring, including: amending its administrative safeguards (such as protocols, practices, procedures, and policies); amending its technological safeguards; and updating its employee training materials.

We are hopeful the above provides sufficient information concerning the incident and Railey Vacation's response. Should you have any questions or concerns regarding this matter, please do not hesitate to contact us. We are available to discuss at your convenience.

Sincerely,

Troutman Pepper Locke LLP



By: _____

Sadia Mirza

Direct: 949.622.2786

Email: sadia.mirza@troutman.com

EXHIBIT A



Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line



Notice of Data Breach



Railey Vacations is writing to inform you of an incident involving your personal information. We encourage you to read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information. Railey Vacations is the trade name for Towne Vacations Deep Creek, LLC.

What Happened?

On October 11, 2024, Railey Vacations became aware of suspicious activity involving an employee's email account. Railey Vacations promptly launched an investigation with the assistance of third-party cybersecurity specialists. The investigation revealed that an unauthorized person gained access to the employee's email account and the emails within it.

What Information was Involved?

We completed a review of the employee's email account to determine what information was involved. The specific information affected varies for each individual. In your case, the information involved includes your name and <<Breached Elements>>.

What Are We Doing?

After detecting the suspicious activity, we promptly secured the affected email account and began an investigation to understand the nature and extent of the incident. We are now notifying those affected individuals and providing them with information and resources to help protect their information. These resources include 24 months of complimentary identity protection services through **Equifax Complete™ Premier**. Additional information pertaining to these services and enrollment instructions are provided below.

1. Register for Complimentary Identity Protection Services with Equifax Complete™ Premier.

Go to www.equifax.com/activate. Enter your unique Activation Code of <<ACTIVATION CODE>> by <<ENROLLMENT DEADLINE>>. Click "Submit" and follow these 4 steps:

- i. **Register:** Complete the form with your contact information and click "Continue".
If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
- ii. **Create Account:** Enter your email address, create a password, and accept the terms of use.

- iii. **Verify Identity:** To enroll in your product, Equifax will ask you to complete its identity verification process.
- iv. **Checkout:** Upon successful verification of your identity, you will see the Checkout Page. Click ‘Sign Me Up’ to finish enrolling.

You’re done! The confirmation page shows your completed enrollment. Click “View My Product” to access the product features.

Key Features

**Note: You must be over age 18 with a credit file to take advantage of the product*

- Annual access to your 3-bureau credit report and VantageScore¹ credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring² with email notifications of key changes to your credit reports
- WebScan notifications³ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts,⁴ which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock⁵
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft.⁶
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

2. **Review Your Accounts for Suspicious Activity.** We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.
3. **Order a Credit Report.** If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at (877) 322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.
4. **Contact the Federal Trade Commission, Law Enforcement and Credit Reporting Agencies.** You may contact the Federal Trade Commission (“FTC”), your state’s Attorney General’s office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s websites at www.identitytheft.gov and www.ftc.gov/idtheft; call the FTC at (877) ID-THEFT (877-438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

¹ The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness

² Credit monitoring from Experian and TransUnion will take several days to begin.

³ WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

⁴ The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

⁵ Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.co

⁶ The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

You may contact the nationwide credit reporting agencies at:

- a) **Equifax:** (888) 378-4329; P.O. Box 740241, Atlanta, Georgia, 30374; or www.equifax.com
- b) **Experian:** (888) 397-3742; P.O. Box 9701, Allen, TX 75013; or www.experian.com
- c) **TransUnion:** (800) 916-8800; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022; or www.transunion.com

5. **Additional Rights Under the Fair Credit Reporting Act.** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the credit reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; credit reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here.

Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf or by writing to Consumer Financial Protection Bureau, 1700 G Street, NW, Washington, DC 20552.

6. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

To place a fraud alert, call any one of the three major credit reporting agencies at the numbers listed below. As soon as one credit reporting agency confirms your fraud alert, they will notify the others. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

(800) 525-6285

Experian

P.O. Box 9554

Allen, TX 75013

<https://www.experian.com/fraud/center.html>

(888) 397-3742

TransUnion LLC

P.O. Box 6790

Fullerton, PA 92834

<https://www.transunion.com/fraud-alerts>

(800) 680-7289

If you are very concerned about becoming a victim of fraud or identity theft, you may request a “Security Freeze” be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the credit reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(800) 349-9960

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>

(888) 397-3742

TransUnion Security Freeze

P.O. Box 2000

Chester, PA 19016

<http://www.transunion.com/creditfreeze>

(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

If you do place a security freeze prior to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

7. **For Maryland Residents.** You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.
8. **For North Carolina Residents.** You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.
9. **For Washington, D.C. Residents.** You can obtain information about avoiding identity theft from the Office of the Attorney General for the District of Columbia at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, DC 20001, (202)-727-3400, www.oag.dc.gov. You have the right to request a security freeze (without any charge) as described above.

Other Important Information.

Railey Vacations established a dedicated call center for individuals to call with any questions or concerns relating to the incident. The phone number is [REDACTED] and representatives are available 9:00am to 9:00pm Eastern. We sincerely regret the inconvenience this incident has caused and remain committed to the security of information in our care.

Sincerely,

Railey Vacations