CONSTANGY
Brooks Smith & Prophete

Nicholas Daly
20 North Wacker
Suite 4120
Chicago, Illinois 60606
ndaly@constangy.com
312.459.6614

Emergency: BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

May 5, 2026

VIA U.S. MAIL
Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents Travelopia Holdings Limited ("Travelopia") in connection with an incident described in greater detail below. Travelopia is an experiential travel company headquartered in the United Kingdom. Travelopia is submitting this letter as a good faith effort to notify your office consistent with any reporting requirements Travelopia could have under N.H. Rev. Stat. § 359-C:20. By providing this notice, Travelopia does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data breach notification statute, or personal jurisdiction.

1. Nature of the Incident

On October 3, 2025, Travelopia became aware of unusual activity within its digital environment. Travelopia immediately took steps to secure its network and initiated an investigation with the assistance of cybersecurity experts. As a result of that investigation, Travelopia learned that certain files may have been accessed and/or acquired without authorization on or about October 2-3, 2025. Travelopia then undertook a comprehensive review of those files in order to determine whether they contained personal information and, on April 1, 2026, learned that New Hampshire residents' personal information was contained within the potentially affected data.

The information involved may vary by individual, but could have included New Hampshire residents' names in combination with a Social Security number or driver's license number.

2. Number of Affected Residents

On April 8, 2026, Travelopia notified two (2) New Hampshire residents by USPS First Class Mail via the attached notification letter or a substantially similar version thereof.

3. Steps Taken Relating to the Incident

Upon discovering the incident, Travelopia conducted a prompt and comprehensive investigation to confirm the scope of the incident. Travelopia has implemented additional measures to further harden its environment and reduce the risk of a similar incident occurring in the future.

Travelopia is notifying the affected New Hampshire residents and providing resources and steps they can take to help protect their information. The notification letter also offers residents the opportunity to enroll in complimentary identity protection services, including 24 months of complimentary credit monitoring and identity protection services, $1 million identity theft insurance, and proactive fraud assistance through Kroll.

4. Contact Information

Travelopia takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 312.459.6614 or ndaly@constangy.com.

Sincerely,

Nicholas Daly

Nicholas Daly
Constangy, Brooks, Smith & Prophete, LLP

Encl. Sample Consumer Notice

Sunsail

The Moorings
Est. 1969

<<First Name>> <<Last Name>>
<<Address1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>>, <<State>> <<Zip Code>>

April 8, 2026

Subject: Notice of Data Incident

Dear <<Title>> <<Last Name>>

This letter is to inform you of a recent data security incident experienced by Travelopia Group Holdings Limited, the UK parent company of Mariner International Travel, Inc d/b/a Sunsail, The Moorings & Leopard Catamarans that may have involved your personal information. We take the privacy and security of all information within our possession very seriously. Please read this letter carefully as it contains information about the incident and resources that you can use to help protect your personal information.

What Happened. In October 2025, we became aware of a potential data security incident on our systems . We immediately took steps to secure the network and initiated an investigation with the assistance of cybersecurity experts. As a result of the investigation, we learned that certain files may have been accessed and/or acquired without authorization for a limited period between October 2-3, 2025. We undertook a comprehensive review of those files and, on or about 1 April 2026, learned that some of your personal information was contained within the potentially affected data.

What Information Was Involved. The information may have included your name as well as your <<DataElements>>.

What We Are Doing. As soon as we discovered this incident, we took the steps described above. We also implemented additional measures to further secure the environment and reduce the risk of a similar incident occurring in the future.

In addition, out of an abundance of caution, we have secured the services of Kroll to provide credit and identity monitoring services at no cost to you for 24 months. 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. Your identity monitoring services include Credit Monitoring, Dark Web Monitoring, Fraud Consultation, and Identity Theft Restoration.

1. You must activate your identity monitoring services by 30 June 2026. Your Activation Code will not work after this date.
2. Visit Enroll.krollmonitoring.com/redeem to activate your identity monitoring services.
3. Provide Your Activation Code: <<Enter Activation Code>> and Your Verification ID: SF-013775.

For more information about Kroll and your Credit and Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

What You Can Do. You can follow the recommendations on the following page to help protect your personal information. You can also enroll in the complementary services offered to you through Kroll by following the instructions set out above.

For More Information. Further information about how to protect your personal information appears on the following page. We would like to reassure you that the safety and security of the data we hold on your behalf remains our priority. This incident affected a small number of people who we are contacting individually. Should you have any questions please write to us at the following email address dataquery@sunsail.com or dataquery@moorings.com or call 1 (844) 403-4578 Monday through Friday from 9am to 5.00pm (noting the call center may be closed on public holidays).

Yours Sincerely,

Laura Fapohunda

Laura Fapohunda
Data Protection Officer – Sunsail/The Moorings

Steps You Can Take to Help Protect Your Personal 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 (the "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 www.annualcreditreport.com, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. 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 www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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. 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 fraud alerts, security freezes, and 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.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov
877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
www.marylandattorneygeneral.gov/Pages/CPD
888-743-0023

Oregon Attorney General
1162 Court St., NE
Salem, OR 97301
www.doj.state.or.us/consumer-protection
877-877-9392

California Attorney General
1300 I Street
Sacramento, CA 95814
www.oag.ca.gov/privacy
800-952-5225

New York Attorney General
The Capitol
Albany, NY 12224
800-771-7755
ag.ny.gov

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
www.riag.ri.gov
401-274-4400

Kentucky Attorney General
700 Capitol Avenue, Suite 118
Frankfort, Kentucky 40601
www.ag.ky.gov
502-696-5300

NC Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov/protectingconsumers/
877-566-7226

NY Bureau of Internet and Technology
28 Liberty Street
New York, NY 10005
www.dos.ny.gov/consumerprotection/
212.416.8433

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include 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 other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf.

KROLL

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

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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. 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.

Dark Web Monitoring

Dark Web Monitoring 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.

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.