Kennedys

22 Vanderbilt Avenue
Suite 2400
New York, NY 10017
USA

**t** +1 646.625.4030
**f** +1 212.832.4920

**kennedyslaw.com**

**t** +1 917.523.3034
Daniel.Marvin@kennedyslaw.com

April 21, 2026

**By Online Reporting**

Attorney General Aaron Frey
Office of the Maine Attorney General
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Dear Attorney General Frey:

We represent Beach Properties d/b/a Basin Harbor Resort ("Basin Harbor Resort"), a resort located in Vergennes, Vermont. We write in accordance with the Maine Notice of Risk to Personal Data Act, 10 M.R.S. § 1348 (2005), to report a data event that involved the personal information of 21 residents of Maine. In making this submission, Basin Harbor Resort does not waive its rights or defenses regarding the applicability of Maine law or personal jurisdiction.

On October 20, 2025, Basin Harbor Resort became aware of suspicious activity within its network environment and took immediate action to secure the environment. Basin Harbor Resort engaged our law firm, as well as CFC-Response, a cyber forensics specialist firm, to conduct an investigation into the cause and scope of the incident, which was confirmed to be a ransomware attack. Following the investigation, Basin Harbor Resort learned that data from its network environment was accessed and acquired without authorization by an unknown actor. On October 24, 2025, Basin Harbor Resort confirmed that certain files within that data set contained personal information. Thereafter, Basin Harbor Resort engaged in a data mining process to identify that personal information and to whom it belonged. Following that process, Basin Harbor Resort also engaged in contact information research in order to affect written notification to as many people as possible. On April 14, 2026, after a national-change-of-address (NCOA) search was run by a notification vendor to verify contact information for those persons whose data was involved, Basin Harbor Resort learned that 21 Maine residents' personal information was involved.

Basin Harbor Resort notified 21 Maine residents via U.S. mail on April 20, 2026. The impacted data included individuals' name and Social Security number. Notified individuals were offered an opportunity to enroll in 12 months of complimentary credit monitoring and identity protection services through TransUnion. A sample copy of the notification letter is enclosed.

Kennedys is a trading name of Kennedys CMK LLP. Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

*Kennedys offices, associations and cooperations:* Argentina, Australia, Belgium, Bermuda, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Portugal, Puerto Rico, Russian Federation, Scotland, Singapore, Spain, Sweden, Thailand, United Arab Emirates, United States of America.

Basin Harbor Resort has taken steps in response to the incident to help mitigate the risk of a similar incident occurring in the future, including reviewing its existing security policies and protections and adopting additional security to safeguard against evolving threats moving forward. Basin Harbor Resort also set up a professional call center through TransUnion to assist notified individuals with credit monitoring enrollments and to answer inquiries regarding the event.

Should you have any further questions, please do not hesitate to contact me. Thank you.

Very truly yours,

*/s/Daniel S. Marvin*

**Daniel S. Marvin**

Partner
for Kennedys

Enclosures: Sample Consumer Notification Letter

Beach Properties d/b/a Basin Harbor Resort
c/o Cyberscout
[redacted]

Basin Harbor
RESORT & BOAT CLUB

April 20, 2026

**Re: Notice of Data Privacy Incident**

Dear [redacted]:

Beach Properties d/b/a Basin Harbor Resort takes privacy and security very seriously. As part of that commitment, we write to notify you of a data security incident involving your personal information. This notice explains the incident, our response, and steps one may take for added protection of personal information, if desired. We are also offering the opportunity to enroll in complimentary credit monitoring and identity protection services.

**What Happened**: On October 20, 2025, we discovered suspicious activity within our network environment. Upon discovery, we took immediate action to secure our network environment and retained cybersecurity professionals to investigate. As part of the investigation, we learned that certain data within our network environment was accessed and acquired by an unauthorized actor on October 20, 2025. As a result, we underwent a comprehensive data review to determine what information may have been involved and to whom that information belonged. As a result of this investigation, we determined that some of your personal information was included in the data set.

**What Information Was Involved:** Our review of the files determined your first and last name, in combination with your [redacted] may have been present within the data set.

**What We Are Doing:** Upon learning of the incident, we took immediate steps to secure our network environment and initiated an investigation with the assistance of cybersecurity professionals. We are also reviewing our policies and existing security controls we have in place to remain resilient against future threats. As added protection, we are offering twelve (12) months of complimentary credit monitoring and identity protection services through TransUnion. Instructions for how to enroll in these services are enclosed.

**What You Can Do:** As a general matter, it is good practice to remain vigilant for incidents of identity theft and fraud, from any source, by reviewing your credit reports and account statements for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider. Please refer to the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional resources you may take advantage of to protect against fraud and identity theft, should you find it appropriate to do so.

**For More Information:** If you have any questions or concerns, please contact our professional assistance line at [redacted], Monday through Friday, 8 a.m. - 8 p.m. Eastern Standard Time, excluding major U.S. holidays. Please know that the security of information is of the utmost importance to us. We remain committed to protecting the information entrusted in our care. We continue to be thankful for your support during this time.

Sincerely,

Basin Harbor Resort

P 0000101102G0500

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

**How to Enroll:**

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

**Monitor Your Accounts and Credit Reports:** It is good practice to remain vigilant of incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

**Fraud Alert Services:** You have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

**Credit Freeze Instructions:** As an alternative to a fraud alert, you have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver's license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

| **TransUnion** | **Experian** | **Equifax** |
|---|---|---|
| 1- 800-916-8800 | 1-888-397-3742 | 1-888-378-4329 |
| www.transunion.com | www.experian.com | www.equifax.com |
| **TransUnion Fraud Alert** | **Experian Fraud Alert** | **Equifax Fraud Alert** |
| P.O. Box 2000 | P.O. Box 9554 | P.O. Box 105069 |
| Chester, PA 19016-2000 | Allen, TX 75013 | Atlanta, GA 30348-5069 |
| **TransUnion Credit Freeze** | **Experian Credit Freeze** | **Equifax Credit Freeze** |
| P.O. Box 160 | P.O. Box 9554 | P.O. Box 105788 |
| Woodlyn, PA 19094 | Allen, TX 75013 | Atlanta, GA 30348-5788 |

**Additional Information:** You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement. Basin Harbor Resort can be reached at [redacted].

*For Maryland Residents*, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; and www.marylandattorneygeneral.gov.

*For 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/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

*For New York Residents*, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; and https://ag.ny.gov.

*For North Carolina Residents*, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

*For Oregon Residents,* the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and https://doj.state.or.us/consumer-protection/.

*For Rhode Island Residents*, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents whose data was impacted by this incident.

P 000010202800000