Maria Efaplomatidis
45 Main Street
Suite 206
Brooklyn, NY 11201
mefaplomatidis@constangy.com
917.414.8991

May 15, 2026

VIA ONLINE PORTAL
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete, LLP represents Vacation Myrtle Beach and its affiliated entities, Legacy Business Solutions LLC and Enjoi Resort, Inc. (collectively, "VMB"), a resort group based out of South Carolina, in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute.

Nature of the Security Incident

On or about June 16, 2025, VMB became aware of suspicious activity in its network environment. In response, VMB immediately took steps to secure its network and launched an investigation with the assistance of forensic experts to determine whether sensitive or personal information may have been accessed or acquired during the incident. As a result of the investigation, VMB identified that certain data may have been acquired without authorization. VMB then engaged an independent team to conduct a comprehensive review of the data involved, and on February 12, 2026, that review determined that certain personal information may have been within the affected data. VMB then worked diligently to identify contact information to effectuate notification and prepare the identity protection services being offered. This process was completed on March 4, 2026.

The information affected varied between individuals but may have included name, Social Security number, driver's license number or state identification number, financial account information, and passport number. Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved in the incident to perpetrate identity theft.

Number of Maine Residents Involved

On May 15, 2026, VMB notified four (4) Maine residents of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

In response to the incident, VMB is providing individuals with information about steps that they can take to help protect their personal information, and, out of an abundance of caution, it is also offering eligible individuals complimentary credit monitoring and identity protection services through Cyberscout Identity Force, a TransUnion company specializing in fraud assistance and remediation services. This includes 12 months of credit and dark web monitoring, a $1,000,000 identity theft insurance policy, and identity protection and resolution services. Additionally, to help reduce the risk of a similar future incident, VMB has implemented additional technical security measures throughout the environment.

Contact Information

VMB remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at MEfaplomatidis@Constangy.com.

Sincerely,

Maria Efaplomatidis
Partner, Constangy Cyber Team

Enclosure: Sample Notification Letter

0006562

Legacy Business Solutions LLC and Enjoi Resort, Inc.
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS3274

26_0006562

[redacted]

To Enroll, Please Visit
https://bfs.cyberscout.com/activate

Enrollment Code: [redacted]

May 15, 2026

Re: Notice of Data Security Incident

Dear [redacted],

We are writing to inform you of a recent data security incident experienced by Vacation Myrtle Beach and its affiliated entities, Legacy Business Solutions LLC and Enjoi Resort, Inc. (collectively, "VMB") that may have involved your personal information. At VMB, we take the privacy and security of all information within our possession very seriously. This is why we are notifying you of the incident, providing you with steps you can take to help protect your personal information, and offering you the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On June 16, 2025, VMB became aware of suspicious activity in its network environment. We immediately took steps to ensure the security of our internal systems and launched an investigation with the assistance of independent forensic exports to determine what happened and what data might have been affected during the incident, if any. As a result of the investigation, we learned that certain data may have been acquired without authorization. VMB then engaged an independent team to conduct a comprehensive review of those files, and on February 12, 2026, that review determined that certain personal information may have been involved. VMB then worked diligently to identify contact information to effectuate notification and prepare the services being offered to affected individuals, as provided in more detail below. This process was completed on March 4, 2026.

What Information Was Involved? The information involved may have included your name, [redacted] **Please note that we have no current evidence to suggest the misuse or attempted misuse of your personal information.** Nonetheless, out of an abundance of caution, we are notifying you of this incident and offering resources to help you protect your personal information.

What We Are Doing. As soon as VMB learned of the incident, we took the measures described above and implemented additional security features to reduce the risk of a similar incident occurring in the future. We are also providing you with information about steps you can take to help protect your personal information.

Additionally, we are offering you the opportunity to enroll in complimentary identity protection services. Specifically, these include Single Bureau Credit Monitoring services at no charge. These services provide you with alerts for 12 months from the date of enrollment when changes occur to your credit file. This

notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

What You Can Do. Please review this letter carefully, along with the guidance included with this letter about additional steps you can take to protect your information. In addition, we encourage you to enroll in the credit monitoring and identity theft protection services we are offering through TransUnion.

To enroll in Credit Monitoring services at no charge, please go to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted, please provide the following unique code to receive services: [redacted]. Please note that the deadline to enroll is 90 days from the date of this letter. The enrollment requires an internet connection and email 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.

For More Information. If you have questions about the incident, please call TransUnion Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern Time, excluding holidays. Please call the designated help line at 1-877-424-7790 and supply the fraud specialist with your unique code listed above. TransUnion representatives are fully versed on this incident and can answer questions you may have regarding the protection of your personal information.

Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Matt Klugman
Chief Operating Officer
Enjoi Resorts, Inc.
Legacy Business Solutions LLC
d/b/a Vacation Myrtle Beach
1144 Shine Ave
Myrtle Beach, SC 29577

0006562

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
1-833-799-5355
www.transunion.com/get-credit-report

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. For TransUnion: www.transunion.com/fraud-alerts.

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. For TransUnion: www.transunion.com/credit-freeze.

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

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

South Carolina Attorney General
P.O. Box 11549
Columbia, S.C. 29211
scag.gov
1-803-734-3970

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

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

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

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
oag.maryland.gov
1-888-743-0023

New Mexico Attorney General
408 Galisteo Street, Villagra Building
Santa Fe, NM 87501
nmdoj.gov/
505-490-4060

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov/consumer-protection
202-442-9828

Iowa Attorney General
1305 E. Walnut Street
Des Moines, Iowa 50319
www.iowaattorneygeneral.gov
888-777-4590

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

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
riag.ri.gov
401-274-4400
RI Residents Affected: 5

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.