Kennedys

22 Vanderbilt Ave.
Suite 24
New York, NY 10017

kennedyslaw.com

t +1 646 625 4030
Daniel.Marvin@kennedyslaw.com
October 10, 2025

Via E-Mail (DOJ-CPB@DOJ.NH.GOV)

Attorney General John Formella
Office of the Attorney General
New Hampshire Department of Justice
33 Capitol Street
Concord, NH 03301

Re: *Notice of Data Breach*

Dear Attorney General Formella:

We represent Natare Corporation ("Natare") and write to provide notice of a data breach pursuant to N.H. Rev. Stat. § 359-C:20, involving the unauthorized acquisition of personal information concerning one New Hampshire resident. This notice shall not be construed as an admission of jurisdiction, liability, or waiver of any rights or defenses by Natare.

Natare is an Indianapolis-based manufacturer, distributor, and supplier of equipment systems and services for commercial and public swimming pools, water features, and aquatic recreations. On August 13, 2025, Natare experienced a ransomware event that resulted in the encryption of its servers. Upon discovery, Natare took immediate action, including taking its systems offline and retained our firm. We retained an independent forensics firm to assist our investigation in furtherance of providing legal advice to Natare. Natare also reported the incident to federal law enforcement.

The forensics investigation concluded that the unauthorized actor had access to Natare systems for less than three hours. On August 25, 2025, after a thorough review of the data involved, Natare confirmed that the unauthorized actor acquired personally identifiable information. The types of information involved in the incident varied by individual. However, the affected data for the New Hampshire resident included the individual's first and last name, in combination with Social Security number. Notifications were mailed on October 6, 2025 via United States Postal Service First-Class mail. The New Hampshire resident was offered an opportunity to enroll in complimentary 12-month credit monitoring and identity protection services through TransUnion. The services include single bureau credit monitoring, dark web

monitoring, access to a $1M insurance reimbursement policy, and fully managed identity theft recovery services.

Following the incident, Natare strengthened its security posture, taking corrective actions in response the breach including: (a) mandatory password reset for all end-users; (b) implemented additional endpoint detection and continuous monitoring tools; (c) enhanced password requirements for administrators; (d) replaced and installed new firewall tools; and (e) replaced and implemented multi-factor authentication software for virtual private network.

Please let me know if you have any questions.

Very truly yours,

/s/ Daniel Marvin

Daniel Marvin

Partner
for Kennedys

Enclosure

Natare Corporation
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
USBFS1845

0000004

NATARE POOLS

Equipment, Systems, Consulting and Engineering for Swimming Pools, Aquatic Facilities and Water Features

1_0000004

[redacted]

October 6, 2025

Notice of Data Breach

Dear [redacted]:

We are writing to inform you of a data security incident our company suffered that involved your personal information. You are receiving this notice because you were or are a current or former employee of Natare Corp. ("Natare") for which we obtained your information. Natare takes this incident seriously and prioritizes the privacy and security of your personal information. We are providing you with information about the incident, our response, and additional steps you may take to further protect your personal information.

On August 13, 2025, Natare became aware of technical issues related to our server. It was later determined that we experienced a ransomware attack. Upon discovery, we took immediate action, which included taking our systems offline and retaining outside cybersecurity specialists to lead our investigation. We also conducted a detailed review of the data involved in the incident, and determined that your personal information was acquired by an unauthorized actor. The information involved includes your first and last name, in combination with the following data elements: [redacted]. Currently, we have no evidence that your information has been used or will be used to commit fraud. However, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no cost to you. These services provide you with alerts for twelve (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. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed "*Steps You Can Take to Help Protect Your Information*." We also established a professional call center, which will include a trained support team to address inquiries concerning the incident as well. These services will be provided by CyberScout, a TransUnion company, who specialize in fraud assistance and remediation services. The dedicated call center may be reached at 1-800-405-6108, Monday through Friday 8:00am – 8:00pm Eastern Time, excluding major U.S. holidays.

As a general matter, one may remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the

financial institution, health insurance provider, or company.

Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Natare Corp.

Enclosure: *Steps You Can Take to Help Protect Your Information*

0000004

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enrollment in Credit Monitoring Services

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

You may remain vigilant against 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.

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.

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 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 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.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and https://oag.dc.gov/consumer-protection.

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; or www.marylandattorneygeneral.gov.

For New Mexico residents, 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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (vi) 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/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

0000004

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; or 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 reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are no residents from Rhode Island whose personal information was involved in this incident.