2049 Century Park East Suite 2900, Los Angeles, CA 90067 • 310.556.1801

December 13, 2022

Pasha Sternberg
310.229.1335
psternberg@polsinelli.com

VIA E-MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)
The Honorable John M. Formella
Attorney General of the State of New Hampshire
Office of the Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Notification of a Potential Data Security Incident

Dear Attorney General Formella:

We represent Lakeside Software, LLC ("Lakeside") in connection with an incident that may have involved the personal information of fifteen (15) New Hampshire residents. Lakeside is reporting the incident pursuant to N.H. Rev. Stat. § 359-C:19 *et. seq*. This notice will be supplemented, if necessary, with any new significant facts discovered subsequent to this submission. While Lakeside is notifying you of this incident, Lakeside does not waive any rights or defenses relating to the incident, this notice, or the applicability of New Hampshire law on personal jurisdiction.

NATURE OF THE INCIDENT

On October 26, 2022, Lakeside discovered unauthorized connections to certain Lakeside systems. Upon learning of the incident, Lakeside immediately took certain systems offline to contain the incident and prevent further unauthorized access to its network. Lakeside, through Polsinelli, engaged a leading forensic security firm to investigate the incident.

The forensic investigation is ongoing but, on November 21, 2022, Lakeside determined that copies of its employee benefits and payroll files could have been taken from its system as part of the incident. Following a review of these files, Lakeside determined, that the incident may have resulted in unauthorized access to New Hampshire residents' personal information. The information varies by individual but across individuals includes names, dates of birth, Social Security numbers, health insurance identification numbers, compensation details, and/or bank account information.

NUMBER OF RESIDENTS AFFECTED

Lakeside determined that the employee benefits and payroll files contained the personal information for fifteen (15) New Hampshire residents. Lakeside is notifying those individuals via written notification letter today, December 13, 2022. Enclosed is a sample of the notice sent to the New Hampshire residents via first-class United States mail.

STEPS TAKEN RELATING TO THE INCIDENT

As discussed above, upon learning of the incident, Lakeside worked with a forensic firm to assist in its investigation and confirm the security of its computer systems. Lakeside also notified law enforcement. Lakeside is notifying the potentially involved individuals and providing them with twenty-four (24) months of complimentary credit monitoring services through IDX. In the notification letters, Lakeside also provided additional steps individuals can take to protect themselves against fraudulent activity and identity theft. Finally, Lakeside is reviewing its technical safeguards and assessing whether to put in additional appropriate safeguards to protect personal information.

CONTACT INFORMATION

Please contact me if you have any questions or if I can provide you with any further information concerning this matter.

Very truly yours,

Pasha Sternberg

Enclosure

Lakeside Software
Return to IDX:
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

December 13, 2022

RE: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

Lakeside Software values and respects the privacy of our employees and community and takes seriously the security and confidentiality of the information entrusted to us. We recently discovered a data security incident that involved some of your personal information. This letter provides information about the incident, including steps that we have taken following the discovery of the incident, as well as steps you can take to protect yourself from the potential misuse of your information, if you have not already done so.

What Happened? On October 26, 2022, we discovered unauthorized connections to certain Lakeside systems. We immediately took our network offline to prevent further unauthorized access and began investigating the incident with the help of several leading incident response firms. We also notified law enforcement. We have re-secured the affected systems, and we have taken steps to help prevent a similar incident from happening in the future. As part of our investigation, on November 21, 2022, we learned that it is likely that a copy of Lakeside's employee benefits and payroll files were taken from our system.

What Information Was Involved? We determined that the information varied by individual, but could include your name, date of birth, social security number or other applicable national identification number, local tax identification number, home address, phone number, health insurance identification number, and/or bank account information associated with your Lakeside payroll and salary/compensation details.

What We Are Doing. In addition to investigating the incident, both internally and with the help of a third party forensic firm, we also notified federal law enforcement. We are also taking steps to help prevent a similar incident from occurring in the future. Additionally, we are offering you and the family members we have listed as your dependents with identity theft protection services. These services are being offered through IDX and include: 24 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What You Can Do. While we are not aware of any fraud or misuse of your information, we encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-800-939-4170 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8 am - 8 pm Central Time. Please note the deadline to enroll is March 13, 2023. You can also find more information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

For More Information. For further information and assistance, please call 1-800-939-4170 from 8:00 A.M. – 8:00 P.M. Central Time, Monday through Friday.

We sincerely apologize for any inconvenience or concern this incident might cause. We value the trust you place in us to protect your privacy, and we take our responsibility to safeguard your personal information seriously.

Sincerely,

Suzie Anthony, Chief People Officer
Lakeside Software

Additional Important Information

1. **IDX Identity Protection Enrollment.** Go to https://app.idx.us/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of this letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution and/or the company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

The District of Columbia and Massachusetts law also allow consumers to place a security freeze on their credit reports. A security freeze can be placed without any charge. Residents of other states can place a security freeze for a small fee. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

Equifax Security Freeze	Experian Security Freeze	Trans Union Security Freeze
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094

In order to request a security freeze, you may need to provide the following information:
1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting www.annualcreditreport.com, by 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 can print a copy of the request form at https://www.annualcreditreport.com/manualRequestForm.action.

Alternatively, you may elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is as follows:

Equifax	Experian	TransUnion
1-866-349-5191	1-888-397-3742	1-800-888-4213
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	P.O. Box 9554	P.O. Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. A fraud alert is free and will stay on your credit report for one (1) year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at www.annualcreditreport.com.

Maryland Residents: Maryland residents can contact the Office of the Attorney General to obtain information about steps you can take to avoid identity theft from the Maryland Attorney General's office at: Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, (888) 743-0023, http://www.marylandattorneygeneral.gov/.

New York State Residents: New York residents can obtain information about preventing identity theft from the New York Attorney General's Office at: Office of the Attorney General for the State of New York, Bureau of Consumer Frauds & Protection, The Capitol, Albany, New York 12224-0341; https://ag.ny.gov/consumer-frauds/identity-theft; (800) 771-7755.

North Carolina Residents: North Carolina residents can obtain information about preventing identity theft from the North Carolina Attorney General's Office at: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-5-NO-SCAM (Toll-free within North Carolina); 919-716-6000; www.ncdoj.gov.