



May 26, 2023

Office of the New Hampshire Attorney General
Department of Justice (Consumer Protection)
33 Capitol Street
Concord, NH 03301

To Whom It May Concern:

Pursuant to your state's law, we are notifying your office of a data breach that affected several New Hampshire residents when an unauthorized third-party gained access to a locked file cabinet containing Human Resources documents. Soon after the event occurred, GioMare Group sent affected individuals the attached data breach notice, which provides a brief description of the incident and instructions on how to monitor their accounts and credit report for unusual activity. A summary of the key facts is set forth below.

What Happened: Sometime between May 8, 2023 and May 18, 2023, a locked file cabinet in our office located at 51 Webb Place, Suite 110, Dover, NH 03820 was broken into. There is no indication that any files or documents were removed from the cabinet.

Type of Information: The folders contained documents that included

The Company's Response: Upon discovery, GioMare Group immediately initiated comprehensive efforts to remediate the incident. These efforts include increased security measures to prevent such an event from recurring. Locks have been changed, local police have been notified and all individuals with information in the file cabinet received the attached notice on May 25, 2023.

Please contact us if you have any questions.

Sincerely,
Amy Mulholland
Finance/HR Manager



Corporate: 781-378-2484
Operations: 603-343-2285
www.GioMareGroup.com



GioMare Corporate HQ
146 Front Street, Suite 208
Scituate, MA 02066



GioMare Operations HQ
51 Webb Place, Suite 110
Dover, NH 03820

From: Human Resources
Sent: Thursday, May 25, 2023 4:26 PM
To: Human Resources
Subject: Notification of Data Breach
Attachments: Information about Identity Theft Protection.pdf

Good afternoon,

We are writing to inform you about a situation that may have exposed some of your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances, steps we are taking in response, and resources we are making available to you.

What Happened?

Sometime this month (May 2023) a locked file cabinet was broken into, in our Dover, NH office. At this time, there is no indication that any documentation was taken from the office. Nevertheless, we are providing this notice out of an abundance of caution since your information was available to the individual who broke into the file cabinet. The rest of the office was fully intact; this file cabinet seems to be the only thing targeted.

What Information Was Involved?

Information that may have been accessed includes

What We Are Doing

Upon discovery of the break-in, we notified local police, and they will be working with the building management to view security footage. All unnecessary documents have been shredded and the locks on the office have been changed to avoid any future incidents. The New Hampshire Attorney General will be notified of the data breach today.

What You Can Do

We want to make sure you are aware of steps you may take to guard against potential identity theft or fraud. Please review the attached "Information about Identity Theft Protection" for information about what you can do.

For More Information

If you have further questions or concerns about this matter, please don't hesitate to reach out to [redacted]. If anyone has any information about this incident that may help with an arrest, please contact us as soon as possible.

We sincerely regret any inconvenience or concern caused by this incident.

Thanks,

Finance/HR Manager

GioMare Group LLC

This e-mail and any files transmitted with it are GioMare Group, LLC property, are confidential, and are intended solely for the use of the individual or entity to whom this e-mail is addressed. If you are not one of the named recipient(s) or otherwise have reason to believe that you have received this message in error, please notify the sender and delete this message immediately from your computer. Any other use, retention, dissemination, forwarding, printing, or copying of this e-mail is strictly prohibited.

Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and **immediately report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities**, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Identity Theft Clearinghouse

600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.identitytheft.gov and www.ftc.gov/idtheft You can also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from <http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idth04.pdf>.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us/idtheft/index.htm
Or contact the Identity Theft Unit directly:
2000 St. Paul Place, 16th Floor, Baltimore, MD 21202, 410-567-6491

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

For residents of Vermont: You may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.

Information about personal health information and medical records

We recommend that you regularly review the explanation of benefits statement that you receive from your insurer. If you see any service that you believe you did not receive, please contact your insurer at the number on the statement. If you do not receive regular explanation of benefits statements, contact your provider and request them to send such statements following the provision of services in your name or number.

You may want to order copies of your credit reports and check for any medical bills that you do not recognize. If you find anything suspicious, call the credit reporting agency at the phone number on the report. Keep a copy of this notice for your records in case of future problems with your medical records. You may also want to request a copy of your medical records from your provider, to serve as a baseline. If you are a California resident, we suggest that you visit the web site of the California Office of Privacy Protection at www.privacy.ca.gov to find more information about your medical privacy.

Suggestions if You Are a Victim of Identity Theft:

- **File a police report.** Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- **Contact the U.S. Federal Trade Commission (FTC).** The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by



calling the FTC's Identity Theft Hotline: 1- 877-IDTHEFT (438-4338); online at <http://www.ftc.gov/idtheft>; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

- **Keep a record of your contacts.** Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In other situations, the cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.*

Because the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

The credit reporting agencies have three 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 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. You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.