

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

September 23, 2022

VIA E-MAIL: IDTheft@oag.state.md.us

Attorney General Brian Frosh
Office of the Maryland Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Notice of Data Breach

Dear Attorney General Frosh:

This notice is provided on behalf of my client, Dirigo Management Company (“Dirigo”), following a data breach that involved the name, date of birth, address, and Social Security number of one (1) Maryland resident. Dirigo is a property management company based in Portland, Maine. Dirigo will provide written notice to this individual later today, via U.S. Mail. The notice letter includes general advice on how to protect one’s identity and obtain free credit reports and security freezes, as well as instructions for enrolling in a one-year, complimentary membership with Experian for credit monitoring and identity theft services. A copy of the notice letter is enclosed and additional details on the incident are below.

In June of 2022, Dirigo learned that some of its clients had received emails from a Dirigo email account that were not authorized. Dirigo began a prompt investigation of the incident, including the engagement of legal counsel with an expertise in cyber security. Legal counsel subsequently retained a nationally-recognized digital forensics and cyber security firm to assist with the investigation so that Dirigo could better understand what happened and, more importantly, help prevent something like this from happening again. After working diligently for several weeks to determine the nature and scope of the incident, the investigation revealed that four Dirigo email accounts had been intermittently accessed without authorization. As soon as Dirigo discovered this, it began a thorough review of the contents of the compromised email boxes in order to determine who may have been affected, what information may have been involved, and where those people reside so that Dirigo could provide proper notice. On August 24, 2022, Dirigo learned that the affected email boxes contained personal information of one (1) Maryland resident.

Dirigo is committed to making this right and is investing in internal processes, tools, and resources to reduce the likelihood that this could happen again. Because cyber threats are always evolving, Dirigo is continuously working to identify and mitigate threats and evaluate its IT security protocols to make sure that sensitive data is protected. In addition, to help prevent similar occurrences in the future, Dirigo has taken the following steps:

1. Closely monitoring and restricting outside access to its systems;
2. Increasing password complexity requirements;
3. Expanding multi-factor authentication to additional employee accounts;
4. Enhancing network intrusion detection and response;
5. Strengthening email filtering to help block dangerous emails; and
6. Enhancing its cyber training and providing regular communications in order to increase cyber awareness.



In addition, consistent with its compliance obligations and responsibilities, Dirigo is providing notice of this incident to appropriate state regulators.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade, Esq.

MHM/
Enclosure



**DIRIGO
MANAGEMENT
COMPANY**

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

NOTICE OF DATA SECURITY INCIDENT

Dear <<Name 1>>:

We are writing to tell you about a recent data security incident involving unauthorized access to four Dirigo Management Company ("Dirigo") employee email boxes. As a result of our investigation, we determined that the email accounts contained personal information about some of our employees, clients, and other individuals affiliated with Dirigo. We take this matter very seriously because we know how important your personal information is to you. We are providing this notice to you as a precautionary measure, to inform you of the incident, explain the complimentary services we are offering you, and suggest ways that you can help protect your information.

What Happened

In June of 2022, we learned that some of our clients had received emails from a Dirigo email account that were not authorized. We immediately launched an investigation with our IT provider and then engaged legal counsel. Legal counsel subsequently hired a nationally recognized digital forensics firm to assist so that we could better understand what happened and, more importantly, prevent something like this from happening again. After working diligently to investigate, we learned that four Dirigo email accounts had been intermittently accessed without authorization. We then worked with counsel and our cybersecurity experts to review the contents of the affected email boxes so that we could find out what, and whose, information was involved. On August 24, 2022, we learned that the affected email boxes contained personal information. We then located mailing addresses for those individuals so that we could notify them of the incident.

What Information Was Involved

Through our investigation, we determined that your name, address, date of birth, Social Security number, or driver's license number were potentially accessed by unauthorized individuals.



Individual Member



ONE CITY CENTER, PORTLAND, MAINE 04101-4009
TEL: (207) 871-1080 · 1-800-615-1080 · FAX: (207) 871-7189
E-MAIL: info@dirigomgmt.com
WEB SITE: www.dirigomgmt.com

What We Are Doing About It

As soon as we discovered this incident, we disabled the affected email accounts, reset passwords, and scanned our email system to detect and terminate unauthorized activity. To further enhance our security and help prevent similar occurrences in the future, we have taken the following steps:

1. Closely monitoring and restricting outside access to our systems;
2. Increasing password complexity requirements;
3. Expanding multi-factor authentication to additional employee accounts;
4. Enhancing network intrusion detection and response;
5. Strengthening our email filtering to help block dangerous emails; and
6. Enhancing our cyber training and providing regular communications in order to increase cyber awareness.

In addition, consistent with our compliance obligations and responsibilities, we are providing notice of this incident to appropriate state regulators.

What You Can Do

We recommend that you take the following preventative measures to help detect and mitigate any misuse of your information.

1. Enroll in a complimentary, one-year membership with Experian. This membership will provide you with identity monitoring services, including a copy of your credit report at signup; credit monitoring; identity restoration; Experian IdentityWorks ExtendCARE; and up to \$1 million in identity theft insurance. Instructions on how to activate your membership are included at the end of this letter.
2. Remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and free credit reports for any unauthorized or suspicious activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter.
3. Report any incidents of suspected identity theft to your local law enforcement, state Attorney General and the major credit bureaus.

For More Information

We are very sorry this incident happened and for any inconvenience you may have experienced. The privacy and security of your information is important to us, and we remain committed to protecting it. If you have any questions or concerns about this incident, you may call us at (207) 871-1080, Monday through Friday, 9 A.M. to 5 P.M. Eastern Standard Time (excluding major U.S. holidays).

Sincerely,



Bob Keegan
President
Dirigo Management Company

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit <https://www.experian.com/blogs/ask-experian/category/fraud-and-identity-theft/> for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

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

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at <https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/articles/pdf/pdf-0093-annual-report-request-form.pdf> and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Colorado, Maine, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

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 90 days. 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. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
www.oag.state.md.us/Consumer
Toll-free: 1-888-743-0023

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at:

Office of the Attorney General Consumer Protection Division
9001 Mail Service Center
Raleigh, NC 27699-9001
<https://ncdoj.gov/contact-doj/>
Phone: 919-716-6000

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State
Division of Consumer Protection
1-800-697-1220

New York Attorney General
1-800-771-7755
<http://www.ag.ny.gov/home.html>

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

TO ACTIVATE YOUR MEMBERSHIP AND START MONITORING YOUR PERSONAL INFORMATION PLEASE FOLLOW THE STEPS BELOW:

- Ensure that you **enroll by:** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** <<Activation Code>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **1-877-288-8057** by <<Enrollment Deadline>>. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian. A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **1-877-288-8057**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.