

February 29, 2024

VIA EMAIL (Idtheft@oag.state.md.us)

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

Re: Northgate Environmental Management, Inc. – Incident Notification

To Whom It May Concern:

McDonald Hopkins PLC represents Northgate Environmental Management, Inc., (“Northgate”) of Oakland, California. I am writing to provide notification of an incident that may affect the security of personal information of twelve (12) Maryland residents. By providing this notice, Northgate does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On March 25, 2023, Northgate detected unauthorized access to its network. Upon learning of this issue, Northgate immediately took steps to secure the environment, and commenced a prompt and thorough investigation. As part of the investigation, Northgate engaged the services of external cybersecurity professionals specifically experienced in handling these sorts of incidents. Along with these cybersecurity experts, Northgate investigated the extent of the incident and what, if any, sensitive data may have been accessed and/or acquired by the unauthorized party.

After an extensive forensic investigation and manual document review, Northgate discovered on or about January 30, 2024, that some limited personal information of the aforementioned Maryland residents was contained in the single email account. Specifically, the information for the Maryland residents included full name, Social Security number, driver’s license number, and financial account number with access code. Not all information was impacted for all Maryland residents.

Northgate has no indication that any of the information has been used for identity theft or financial fraud. Nevertheless, out of an abundance of caution, Northgate wanted to inform your Office of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Northgate is providing the affected residents with written

August 24, 2023

Page 2

notification of this incident commencing on or about February 29, 2024, in substantially the same form as the letter attached hereto. The individuals will be offered complimentary credit monitoring services. Northgate will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Additionally, the affected residents will also be provided with the contact information for the consumer reporting agencies, the Maryland Attorney General, and the Federal Trade Commission.

At Northgate, protecting the privacy of personal information is a top priority. Northgate is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it.

If you have any additional questions, please contact me at (312) 642-6131 or bdawson@mcdonaldhopkins.com.

Very truly yours,

A handwritten signature in black ink, appearing to be 'BLD', followed by a long horizontal flourish.

Blair L. Dawson, JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM

Encl.

[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

The privacy and security of the personal information we maintain is of the utmost importance to Northgate Environmental Management, Inc. ("Northgate"). We are writing with important information regarding a recent security incident that may have impacted some of your information. We want to provide information about the incident, explain the services we are making available to you and let you know that we continue to take significant measures to protect your information.

What Happened?

On or about March 25, 2023, Northgate detected unauthorized access to our network environment.

What We Are Doing.

Upon learning of this issue, Northgate immediately took steps to secure our network environment and commenced a prompt and thorough investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals experienced in handling these types of incidents. Following this thorough investigation and our manual document review, we learned on January 30, 2024, that certain files containing personal information may have been subject to unauthorized access or acquisition.

What Information Was Involved?

The impacted data contained some of your personal information, including your full name and [REDACTED]

What You Can Do.

We have no evidence that any of your information has been used for identity theft or financial fraud as a result of this incident. Nevertheless, we are offering a complimentary 12-month membership of Experian IdentityWorksSM Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary 12-month membership, please see the additional information provided in this letter.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis. To the extent that it is helpful, we have included information about protecting against medical identity theft.

For More Information.

Please accept our apologies that this incident occurred. Northgate is committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. Northgate continually evaluates and modifies its practices and internal controls to enhance the security and privacy of your personal information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED] This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, [REDACTED]

Sincerely,

Northgate Environmental Management, Inc.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. Ensure that you **enroll by** [REDACTED] (Your code will not work after this date.)
2. **Visit** the Experian IdentityWorks website to enroll: [REDACTED]
3. Provide your **activation code:** [REDACTED]

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [REDACTED]. Be prepared to provide engagement number [REDACTED] as proof of eligibility for the Identity Restoration services by Experian.

**ADDITIONAL DETAILS REGARDING YOUR
12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

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 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.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at [REDACTED]
[REDACTED] to register with the activation code above.**

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at [REDACTED]

* 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.

2. Obtain and Monitor Your Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the three major nationwide credit reporting companies. You can obtain a free copy of your credit report by calling **1-877-322-8228**, visiting **www.annualcreditreport.com**, 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 access the request form at <https://www.annualcreditreport.com/index.action>. Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

3. Placing a Fraud Alert on Your Credit File.

Whether or not you choose to use the complimentary credit monitoring services, we recommend that you place an initial 1-year “fraud alert” on your credit files, at no charge. An initial fraud alert is free and will stay on your credit file for at least twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>.

Equifax

P.O. Box 105069
Atlanta, GA 30348-5069
<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>
(800) 525-6285

Experian

P.O. Box 9554
Allen, TX 75013
<https://www.experian.com/fraud/center.html>
(888) 397-3742

TransUnion

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19016-2000
<https://www.transunion.com/fraud-alerts>
(800) 680-7289

4. Placing a Security Freeze on Your Credit File.

Following is general information about how to request a security freeze from the three credit reporting agencies at no charge. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. 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. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided below). You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348-5788

<https://www.equifax.com/personal/credit-report-services/credit-freeze/>

(888) 298-0045

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

<http://experian.com/freeze>e
(888) 397-3742***TransUnion Security Freeze***

P.O. Box 160

Woodlyn, PA 19094

<https://www.transunion.com/credit-freeze>

(888) 909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information. 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.

5. Protecting Your Medical Information.

We have no evidence that your medical information involved in this incident was or will be used for any unintended purposes. However, the following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your “explanation of benefits statement” which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

6. Additional Helpful Resources.

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 on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC’s Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

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.

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

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal
As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail

Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.