BakerHostetler

Baker&Hostetler LLP
1170 Peachtree Street
Suite 2400
Atlanta, GA 30309-7676
T 404.459.0050
F 404.459.5734
www.bakerlaw.com

John P. Hutchins
direct dial: 404.946.9812
jhutchins@bakerlaw.com

September 24, 2021

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Primland Ltd. ("Primland"), to notify you of a security incident involving two New Hampshire residents.

Primland recently concluded an investigation of an incident that involved unauthorized access to five employees' email accounts. Upon first learning of the potential access to the employees' email accounts, Primland launched an investigation with the assistance of a cybersecurity forensics firm.

Through this investigation, completed on June 7, 2021, Primland discovered that an unauthorized party gained access to the employees' email accounts between December 2, 2020 and December 10, 2020, and on May 25, 2021. The investigation was unable to determine whether the unauthorized party viewed any emails or attachments in the accounts. In an abundance of caution, Primland reviewed the emails and attachments contained in the email accounts to identify individuals whose personal information may have been accessible to the unauthorized party. Through that review, Primland identified emails and/or attachments containing the names and credit or debit card numbers, and/or medical information of two New Hampshire residents.

On September 24, 2021, in accordance with N.H. Rev. Stat. Ann. § 359-C:20,[1] Primland is providing written notice via United States Postal Service mail to the two New Hampshire residents whose personal information was potentially accessed by an unauthorized party. The notice letter provides a telephone number that notice recipients can call with any questions they may have.

[1] This notice does not waive Primland Ltd.'s objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this incident.

To help prevent a similar incident from occurring in the future, Primland has implemented measures to enhance their existing security, including moving the on premises email system to the cloud, upgrading firewall and antivirus software throughout the network, changing employee email passwords, and are continuing to educate staff on how to identify and avoid malicious emails.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

John P. Hutchins

John P. Hutchins
Partner

Enclosure

PRIMLAND

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>>:

Primland Ltd. understands the importance of protecting the information we maintain. We are writing to inform you of an incident that may have involved some of your personal information. This notice explains the incident, measures we have taken, and some steps you may consider taking in response.

Primland discovered that an unauthorized person accessed five Primland employee email accounts. We took immediate steps to secure the accounts, began an investigation, and a cybersecurity firm was engaged to assist. The investigation determined that an unauthorized person accessed the email accounts between December 2, 2020 and December 10, 2020 and on May 25, 2021. However, the investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the accounts, and we are unable to rule out that possibility. Therefore, we conducted a thorough review of the information potentially accessed, and on June 7, 2021, determined that an email or attachment contained your <<b2b_text_1(Name, Impacted Data)>>.

We encourage you to remain vigilant by reviewing your financial account statements for any unauthorized activity. You should immediately report any unauthorized activity to your financial institution. Further, in an abundance of caution, we are offering you access to Kroll's identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. This service is completely free to you and enrolling in this program will not hurt your credit score. **For more information about Kroll's identity monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:**

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

*You have until **December 21, 2021** to activate your identity monitoring services.*

Membership Number: **<<Membership Number s_n>>**.

For more information on identity theft prevention, additional steps you may consider taking to help protect your personal information, and information on how to activate your complimentary one-year identity monitoring membership, please see the additional information provided with this letter.

To help prevent a similar incident from occurring in the future, we have implemented measures to enhance our existing security and are continuing to educate our staff on how to identify and avoid malicious emails. In addition, we created a dedicated call center to answer any questions you may have about the incident. If you have any questions, please call 1-???-???-????, Monday through Friday, between 8:00 a.m. and 5:30 p.m. Central Time, excluding some U.S. holidays.

Sincerely,

Steve Helms

Steve Helms
Vice President

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts 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 one year. 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.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

***Credit or Security Freezes*:** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with 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.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Maryland: You can contact the Primland by mail at 2000 Busted Rock Road, Meadows of Dan, VA 24120. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You can contact the Primland by mail at 2000 Busted Rock Road, Meadows of Dan, VA 24120 or by telephone at 276-222-3801. You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

Washington: On or about December 9, 2020, Primland discovered that an unauthorized person had accessed email accounts of certain Primland employees. On June 7, 2021, Primland learned that the personal information of Washington residents was involved in the incident.

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.