BakerHostetler

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

Daniel A. Pepper
direct dial: 215.564.2456
dpepper@bakerlaw.com

September 28, 2020

STATE OF NH
DEPT OF JUSTICE
2020 SEP 29 PM 12:32

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:

I am writing to notify you of a data security incident on behalf of my client, the Island Institute, a non-profit organization that works to sustain Maine's island and coastal communities, and exchanges ideas and experiences to further the sustainability of communities here and elsewhere.

On August 4, 2020, Island Institute concluded its investigation of an incident that involved unauthorized access to two employees' email accounts. Upon first suspecting unauthorized access to the employees' email accounts, Island Institute immediately reset the passwords to the accounts and launched an investigation.

Through the investigation, Island Institute learned that an unauthorized party gained access to the two employees' email accounts between the dates of May 16, 2020 and June 15, 2020 as a result of the employees responding to a phishing email. The investigation was unable to rule out the possibility that the unauthorized party may have been able to view or access emails and attachments in the accounts. Island Institute therefore conducted a comprehensive review of the emails and attachments contained in the two email accounts and determined that the personal information of 20 New Hampshire residents was in the accounts including their names, Social Security numbers and financial account numbers.

Beginning on September 28, 2020, Island Institute will mail notification letters via U.S. mail to the New Hampshire residents whose personal information may have been involved in this incident,

in accordance with N.H. Rev. Stat. Ann. § 359-C:20.[1] A copy of the notification letter is enclosed. Island Institute is offering one year of complimentary credit monitoring and identity theft protection service through Kroll to eligible individuals whose information may have appeared in the accessed accounts. Island Institute is also providing a call center for the individuals to call with questions regarding the incident.

To help prevent a similar incident from occurring in the future, Island Institute has implemented multifactor authentication on all users' email accounts and conducted additional training for its employees concerning data security.

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

Sincerely,

Daniel A. Pepper
Partner

Enclosure

[1] This notice is not, and does not constitute, a waiver of Island Institute's objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

ISLAND INSTITUTE

<<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>> <<middle_name>> <<last_name>> <<suffix>>,

Island Institute is committed to safeguarding the privacy and security of the information we maintain. We are writing to inform you about a data security incident that may have involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On August 4, 2020, Island Institute concluded its investigation of an incident that involved unauthorized access to two employees' email accounts. Upon first suspecting unauthorized access to the employees' email accounts, we immediately reset the passwords and launched an investigation.

In connection with that investigation, we learned that an unauthorized party gained access to the two employees' email accounts between the dates of May 16, 2020 and June 15, 2020 as a result of the employees responding to a phishing email. Our investigation was unable to rule out the possibility that the unauthorized party may have been able to view or access emails and attachments in the accounts. We therefore conducted a comprehensive review of the emails and attachments contained in the two email accounts and determined that the account included your <<b2b_text_1(ImpactedData)>>.

To date, we are unaware of any misuse of the information maintained in the employees' email accounts. Nor do we have any definitive evidence that any emails or attachments containing your information were actually viewed or accessed. However, out of an abundance of caution, we wanted to let you know this happened and assure you that we take this very seriously. We encourage you to remain vigilant by reviewing your financial account statements for any unauthorized activity. If you see charges or activity you did not authorize, please contact your financial institution immediately. As a precaution, we have arranged for Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on identity theft prevention and Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

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

*You have until **December 22, 2020** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

We deeply regret any concern this incident may cause you. To help prevent a similar incident from occurring in the future, Island Institute has implemented multifactor authentication on all users' email accounts and conducted additional training for its employees concerning data security. If you have any questions, please call our dedicated call center at 1-866-410-0484, Monday through Friday from 9:00am to 6:30pm Eastern Time.

Sincerely,

Peter Rand
Chief Financial Officer

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: 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 Island Institute via U.S. mail at 386 Main Street, Rockland, ME 04841. 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 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
- New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

Rhode Island: This incident involves 3 individuals in Rhode Island. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

Kroll | A Division of DUFF&PHELPS

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 will 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.