



Julie A. Keersmaekers
1700 Lincoln Street, Suite 4000
Denver, CO 80203
Julie.Keersmaekers@lewisbrisbois.com
Direct: 720.292.2047

October 20, 2021

VIA WEBSITE PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330
Email: breach.security@maine.gov

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent Urban Resource Institute (“URI”), a Manhattan-based nonprofit organization that offers shelter and support services for survivors of domestic violence, the homeless, and adults who have been diagnosed with intellectual and developmental disabilities. This letter is being sent because personal information of certain Maine residents was found in accessed email accounts in a data security incident experienced by URI.

On July 23, 2020, URI learned of unusual activity involving an individual employee email account. Upon discovering this activity, URI immediately engaged a team of cybersecurity experts to secure its email environment and to conduct an investigation to determine what happened and whether any personal information was accessed or acquired without authorization. As a result of the investigation, in October of 2020, URI learned that certain employee email accounts were accessed without authorization. Although URI did not discover evidence that sensitive information in the email accounts was accessed or targeted by the unauthorized actor(s), URI decided to conduct a comprehensive review of the contents of the relevant email accounts. Upon conclusion of that review, in late June 2021, URI learned that personal information belonging to individuals, including certain URI employees and clients, was located in the relevant accounts. Although there is no evidence that the personal information identified was itself accessed or acquired without authorization during this incident, URI decided to notify the individuals whose information was found in the affected accounts. URI then worked diligently to identify current address information for the potentially impacted individuals, and coordinated with City and State agencies to prepare for notification. That process was completed on or about October 18, 2021. URI began mailing notification letters on October 20, 2021.

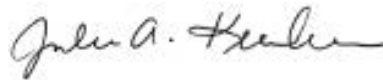
Due to the nature of the services URI provides, traditional notification may present a serious safety risk to the notified population, which includes individuals to whom URI has provided or is providing domestic and family violence services. In particular, notified individuals who reside with a current or former abuser may be at risk should the abuser discover the notified individual sought domestic violence services from URI. In order to provide notice of the incident and access to credit and identity monitoring and protection services, while also mitigating the serious safety risk such notice

may present, URI provided anonymized notification letters that do not therein identify URI as the organization that experienced the incident. Should notified individuals request information about the identity of the organization, such information will be disclosed upon confirmation of the safety of the inquiring notified individual. After careful consideration, URI believes this approach balances the important interests of providing notice of the incident while also prioritizing the safety and security of notification population.

URI notified six (6) Maine residents of this incident via the attached sample letter on October 20, 2021. URI offered notified individuals complimentary credit monitoring and identity theft restoration services through IDX, a global leader in risk mitigation and response. These services include twelve (12) months of credit monitoring and fully managed identity theft recovery services.

Please contact me should you have any questions.

Very truly yours,



Julie A. Keersmaekers
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Consumer Notification Letter

To Enroll, Please Call:
1-833-909-3930
Or Visit:
[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)
Enrollment Code: <<Enrollment>>

<<FirstName>> <<LastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

October 20, 2021

Subject: Notice of Data Security Incident

Dear <<FirstName>> <<LastName>>:

We are writing to tell you about a data security incident experienced by an organization we represent. We learned that one or more unauthorized individual(s) gained access to the email accounts of certain employees of the organization. These accounts may have contained some of your personal information. We have no evidence your information was accessed without permission or misused. However, since we cannot rule out the possibility that someone may have viewed or misused your information without permission, we are writing to:

- Notify you of this incident,
- Offer you free credit monitoring and identity protection services, and
- Inform you of steps you can take to help protect your personal information.

What Happened? On or around July 23, 2020, the organization learned of unusual activity involving an individual employee email account. When we discovered this activity, the organization immediately took steps to secure the account as well as its email environment. The organization also began an investigation.

The organization hired a leading, independent firm with expertise in these matters to determine what happened and if sensitive information was accessed or obtained without permission. As a result of that investigation, in October of 2020, the organization learned that certain employee email accounts were accessed without permission. Although the organization did not discover evidence that sensitive information in the email accounts was accessed or targeted by the unauthorized individual(s), to be extra careful, we then conducted a comprehensive review of the contents of the relevant email accounts.

On June 24, 2021, the organization learned that one or more of the accounts contained some of your personal information. The organization then worked to identify current address information and to provide this notification to you. That process was completed on October 11, 2021, which led to this outreach to you.

What Information Was Involved? The personal information may have included your <<variable1>>, as well as additional information collected in connection with your employment or services provided to you.

What Are We Doing for You? Finally, the organization is giving you information about steps you can take to help protect your personal information. We are also offering you credit monitoring and identity theft restoration services at no cost to you through IDX, a data breach and recovery services expert.

IDX identity protection services include: <<Duration>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What Can You Do? You should review the guidance included with this letter about how to help protect your information. We also encourage you to contact IDX with any questions and to enroll in free identity protection services by calling 1-833-909-3930 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time. The deadline to enroll is January 20, 2022.

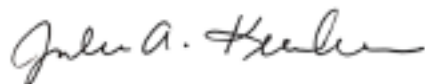
We encourage you to take advantage of this service. IDX representatives know about the incident and can answer questions or respond to concerns you may have about the protection of your personal information.

What Are We Doing To Protect Against Future Incidents? As soon as the organization discovered this incident, we took the steps described above. The organization has also put in place extra safeguards to help ensure the security of its email environment and to reduce the risk of a similar incident happening again. The organization also reported this matter to the Federal Bureau of Investigation (FBI) and will provide whatever help is necessary to hold the person(s) who did this accountable.

For More Information: Further information about how to help protect your personal information appears on the next page. If you have questions or need assistance, please call our dedicated call center at 1-833-909-3930, Monday through Friday from 9:00 am – 9:00 pm Eastern Time.

We take your trust in us, your privacy, and this matter very seriously. We regret any concern or inconvenience that this may cause you.

Sincerely,



Julie A. Keersmaekers of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
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 19016
1-800-916-8800
www.transunion.com

Fraud Alert: 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 one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

**North Carolina Attorney
General**

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

**Rhode Island Attorney
General**

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

**Washington D.C. Attorney
General**

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.