February 15, 2024

VIA EMAIL

Attorney General John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General Formella:

Constangy, Brooks, Smith & Prophete, LLP ("Constangy") represents Urban Resources Institute ("URI"), a social services organization, in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the impact to New Hampshire residents in accordance with New Hampshire's data breach notification statute. URI hereby reserves all rights and defenses in connection herewith.

1. Nature of the Security Incident

On February 11, 2023, URI became aware of unusual activity that disrupted access to certain systems. Upon discovering this activity, URI immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened. Based on that investigation, URI learned that an unknown criminal actor gained unauthorized access to its network and acquired certain files, some of which contained individuals' personal information. URI immediately engaged a third-party vendor to review the affected data to determine whether any sensitive data was involved and whether personal information may have been affected. On January 22, 2024, URI confirmed that personal information belonging to certain New Hampshire residents was involved. URI then took steps to notify those individuals as quickly as possible.

Please note that we have no current evidence to suggest misuse or attempted misuse of personal information involved.

2. Number of Affected New Hampshire Residents & Information Involved

The incident involved personal information for approximately a single (1) New Hampshire resident. The information involved in the incident may have included individuals'

.

3. Notification of Affected Individuals

On February 15, 2024, notification letters were mailed to affected New Hampshire residents by USPS First Class Mail. The notification letter provides resources and steps individuals can take to help protect their information. The notification letter also offers of complimentary identity protection services to each individual whose personal information was affected by this event, including credit monitoring, $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Those services are offered by Experian, a company specializing in fraud assistance and remediation services. Experian will also support a call center for 90 days to answer questions and assist with enrollment. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

3. Steps Taken to Address the Incident

In response to the incident, URI retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. URI also implemented additional security measures to further harden its digital environment in an effort to prevent a similar event from occurring in the future. Additionally, URI has reported the incident to the FBI and will cooperate with any resulting investigation.

Finally, URI is notifying the affected individuals and providing them with steps they can take to protect their personal information as discussed above.

4. Contact Information

URI remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at .

Sincerely,

Lauren Godfrey of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Consumer Notification Letter

CONSTANGY
BROOKS, SMITH &
PROPHETE LLP

Return Mail Processing
PO Box 999
Suwanee, GA 30024

9 1 2418 **********SNGLP
SAMPLE A. SAMPLE - General
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

February 15, 2024

Subject: Notice of Data **[Extra1]**

Dear Sample A. Sample:

We are writing to notify you of a data security incident at an organization we represent, Urban Resource Institute ("URI"). URI learned that an unauthorized person gained access to a URI employee's computer. This computer had some of your personal information saved on it. We are writing to notify you of this incident and to share steps you can take to protect your personal information. URI also wants to offer you free credit monitoring and identity protection services.

What Happened. On or around February 11, 2023, URI discovered that someone outside of URI had gotten access to its network. When URI discovered this activity, they immediately took steps to lock the system down. URI then began an immediate investigation.

URI hired outside experts to determine what happened and if private information was accessed or taken without permission. The investigation did not prove that your private information was accessed or taken by unauthorized people. However, URI continued to investigate to be extra careful. URI then conducted a review of the data contained on the employee's computer. On December 11, 2023, URI finished their review and confirmed that some of your personal information was part of the data that we reviewed.

PLEASE NOTE: URI is not aware of the misuse of any of the information that was part of this incident.

What Information Was Involved. The personal information may have included your

.

What We Are Doing. URI took immediate action to lock down the system and investigate what happened and who was involved. URI has also put in place extra safeguards to help ensure the security of its computer systems. This will reduce the risk of another incident happening again. URI 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.

To help protect your identity, we are offering complimentary access to Experian IdentityWorks^{SM} for **[Extra2]** months.

Please note that Identity Restoration is available to you for [Extra2] months 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.

If you believe that someone has stolen your identity or your credit information, then identity restoration assistance through Experian is immediately available to you. URI also encourages you to use the fraud protection tools available through Experian IdentityWorks. This is a free [Extra2]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need help with Identity Restoration because of this incident, or would like to enroll in Experian IdentityWorks by telephone, please contact Experian's customer care team at . Be prepared to provide engagement number **[Engagement Number]** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra2]-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian now 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 file 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.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

What You Can Do. URI recommends that you start your free services using the enrollment code provided below. URI also recommends that you review the directions included with this letter about how to protect your personal information.

For More Information. URI is very sorry for any stress or concern caused by this incident. If you have further questions, or do not want to enroll online, please call 833-281-4829 toll-free Monday through Friday from 9 am - 9 pm EST (excluding major U.S. holidays). Be prepared to provide your engagement number [Engagement Number].

URI takes your trust in them, your privacy, and this matter very seriously. URI regrets any concern or inconvenience that this may cause you.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Constangy, Brooks, Smith & Prophete, LLP

* 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.

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/sites/default/files/articles/pdf-0096-fair-credit-reporting-act.pdf.