



MULLEN  
COUGHLIN<sub>LLC</sub>  
ATTORNEYS AT LAW

RECEIVED

FEB 25 2020

CONSUMER PROTECTION

Sian M. Schafle  
Office: (267) 930-4799  
Fax: (267) 930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

February 21, 2020

**INTENDED FOR ADDRESSEE(S) ONLY**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Urban Alliance Foundation (“Urban Alliance”) located at 2030 Q Street NW, Washington, DC 20009, and are writing to notify your office of an incident that may affect the security of some personal information relating to one (1) New Hampshire resident. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Urban Alliance does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

Urban Alliance became aware of unusual activity involving certain employee email accounts. Urban Alliance immediately commenced an investigation with the assistance of third-party computer specialists. The investigation determined that the employee email accounts were accessed without authorization between September 10, 2019 and September 12, 2019. Urban Alliance immediately began a thorough review of the contents of the email accounts to determine whether sensitive information was present in the accounts at the time of the incident.

The preliminary results of the email account review indicated that some personal information may have been present in the affected email accounts at the time of the incident. The results, however, contained missing address information and, therefore, there was insufficient information to determine whether the information constituted personal information as defined by N.H. Rev. Stat. Ann. § 359-C:19(IV)(a). Therefore, Urban Alliance reviewed relevant source documents and

[Mullen.law](http://Mullen.law)

internal records to confirm the last known address for potentially affected individuals. On January 7, 2020, Urban Alliance completed this analysis and confirmed that personal information as defined by N.H. Rev. Stat. Ann. § 359-C:19(IV)(a) was present within the relevant email accounts at the time of the incident including the name and financial account number of one (1) New Hampshire resident. Urban Alliance then moved quickly to notify the state resident.

#### **Notice to New Hampshire Resident**

On February 21, 2020, Urban Alliance mailed written notice of this incident to potentially affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*. To date, Urban Alliance is unaware of any actual or attempted misuse of information relating to a New Hampshire resident as a result of this incident.

#### **Other Steps Taken and To Be Taken**

Upon discovering the event, Urban Alliance moved quickly to investigate and to respond to the incident, to assess the security of Urban Alliance systems, and to notify potentially affected individuals. Urban Alliance's response included initiating universal password reset, reviewing the contents of the email accounts to determine whether personal information may have been impacted by this incident, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. Urban Alliance has implemented additional security features to its email accounts and has reassessed account permissions to limit access to certain information stored on its network. Urban Alliance is also providing additional workforce training to its staff. Urban Alliance is providing access to credit and identity monitoring services for two (2) years, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

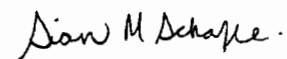
Additionally, Urban Alliance is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Urban Alliance has reported this event to law enforcement.

Office of the New Hampshire Attorney General  
February 21, 2020  
Page 3

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of  
MULLEN COUGHLIN LLC

SMS/dle

# **EXHIBIT A**



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

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

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Urban Alliance Foundation ("Urban Alliance") respects the privacy of your personal information, which is why we are writing to let you know about an incident with some of our email accounts. While there is currently no evidence that your information has been misused as a result of this incident, out of an abundance of caution, we are providing you with information about the incident, our response, and resources available to you to better safeguard your information should you feel it appropriate to do so.

Urban Alliance became aware of unusual activity involving a limited number of employee email accounts. Urban Alliance immediately commenced an investigation with the assistance of computer forensic specialists. The investigation determined that the employee email accounts were accessed without authorization sometime between September 10, 2019 and September 12, 2019. While the investigation did not determine that sensitive information had been viewed by an unauthorized actor, we cannot rule out the possibility of such activity. Therefore, Urban Alliance immediately began a thorough review of the contents of the email accounts to determine whether sensitive information was present in the accounts at the time of the incident.

Urban Alliance received the preliminary results of the email account review which indicated that some personal information may have been present in an affected email account at the time of the incident. On or around January 7, 2020, Urban Alliance completed its review and analysis of this information and our files to determine the identities of those who were potentially involved and their last known address information for purposes of notifying them of this incident. Through this process, we determined that your personal information was present in an email account at the time of the incident. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

Our investigation determined that at the time of the incident, the email accounts contained information including your <<ClientDef1(Impacted Data)>>.

Information, privacy, and security are among our highest priorities. Urban Alliance has strict security measures in place to safeguard information in our care. Upon learning of this incident, we moved quickly to investigate and respond to this incident and confirm the security of our systems, including our email environment. Our response included initiating universal password reset, reviewing the contents of the email accounts to determine whether personal information may have been impacted by this incident, and reviewing internal systems to identify contact information for purposes of providing notice to potentially affected individuals. As part of our ongoing commitment to the security of information we are reviewing and enhancing existing policies and procedures and conducting additional workforce training to reduce the likelihood of a similar future event. We are notifying you in an abundance of caution to ensure you are aware of this incident. As a precautionary matter, we also notified law enforcement and provided relevant regulatory notices.

While, to date, we have no evidence of actual or attempted misuse of your information as a result of this incident, we are notifying you so that you may take further steps to better safeguard your personal information should you feel it is appropriate to do so. We are offering you access to complimentary identity monitoring services for twenty-four (24) months through Kroll. If you wish to activate the identity monitoring services, you may follow the instructions included in the *Steps You Can Take to Help Protect Your Information*.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity and to detect errors. You may also review the information contained in the attached Steps You Can Take to Help Protect Your Information and activate to receive the identity monitoring services we are making available to you. While Urban Alliance will cover the cost of this service, you will need to complete the activation process.

We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at [1-800-888-8888](tel:1-800-888-8888) 8:00 am to 5:30 pm CST Monday through Friday (excluding some U.S. national holidays). You may also write to Urban Alliance at: 2030 Q Street NW, Washington, DC 20009.

Sincerely,

A handwritten signature in black ink that reads "Esha Smith". The signature is written in a cursive, flowing style.

Eshauna Smith  
Chief Executive Officer  
Urban Alliance

## Steps You Can Take to Help Protect Your Information

### Activate in Identity Monitoring

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for two years. 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. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

### Monitor Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/freeze/center.html">www.experian.com/freeze/center.html</a>	<b>TransUnion</b> P.O. Box 160 Woodlyn, PA 19094 1-888-909-8872 <a href="http://www.transunion.com/credit-freeze">www.transunion.com/credit-freeze</a>	<b>Equifax</b> P.O. Box 105788 Atlanta, GA 30348-5788 1-800-685-1111 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	--	---

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

<b>Experian</b> P.O. Box 9554 Allen, TX 75013 1-888-397-3742 <a href="http://www.experian.com/fraud/center.html">www.experian.com/fraud/center.html</a>	<b>TransUnion</b> P.O. Box 2000 Chester, PA 19016 1-800-680-7289 <a href="http://www.transunion.com/fraud-victim-resource/place-fraud-alert">www.transunion.com/fraud-victim-resource/place-fraud-alert</a>	<b>Equifax</b> P.O. Box 105069 Atlanta, GA 30348 1-888-766-0008 <a href="http://www.equifax.com/personal/credit-report-services">www.equifax.com/personal/credit-report-services</a>
---	---	--

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

**For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; or [www.ncdoj.gov](http://www.ncdoj.gov). You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

**For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or [www.oag.state.md.us](http://www.oag.state.md.us).

**For New Mexico residents**, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**For New York residents**, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services<sup>1</sup> from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—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 can help you determine if it's 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 can dig deep to uncover the scope of the identity theft, and then work to resolve it.

<sup>1</sup> 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.