

RECEIVED

APR 20 2020

CONSUMER PROTECTION

**goulston&storrs**  
counselors at law

Christian W. Habersaat  
chabersaat@goulstonstorrs.com  
(617) 574-3549 (tel)  
(617) 574-4112 (fax)

April 16, 2020

Office of the New Hampshire Attorney General  
Gordon J. MacDonald, Attorney General  
33 Capitol Street  
Concord, NH 03301

**Re: Oxfam America Inc.- Data Breach Notification**

Dear Sir/Madam:

This firm represents Oxfam America Inc. (“Oxfam”). We are writing to notify you of a data security incident that *potentially* compromised the security of personal information of approximately twenty-three (23) New Hampshire residents, former and current employees of Oxfam and their family members. Oxfam’s investigation into the event described below is ongoing, and this notice will be supplemented, as is necessary, as any additional material information is learned.

#### **Nature of Data Security Event**

Oxfam is a nonprofit international development and relief organization dedicated to finding lasting solutions to poverty and related injustice. The organization, which maintains its headquarters in Boston, Massachusetts, was the victim of a cyber-attack that resulted in the potential exposure of data, including the personal information of New Hampshire residents, to a party outside of Oxfam.

On March 23, 2020, Oxfam learned that an unauthorized party encrypted and locked down Oxfam’s network, demanding ransom in exchange for restoring Oxfam’s access to certain of its systems. Upon learning of this event, Oxfam immediately engaged LIFARS, a cyber security company, to conduct a forensic investigation into the ransomware attack and to ensure that its network was secure. On or about April 1, 2020, in the course of its investigation, LIFARS determined with a high level of certainty that a Chinese threat actor, APT41, may have penetrated Oxfam’s network infrastructure through ManageEngine, an application used by Oxfam to manage its IT infrastructure. LIFARS further determined that the threat actor used the ransomware attack as a mechanism to cover its tracks. LIFARS advised Oxfam that the attacker’s access to the network likely occurred on March 8, 2020 and any access ended by

March 23, 2020 when Oxfam first learned of the cyber-attack. LIFARS believes that the threat actor was in and out of Oxfam's network quickly.

While neither Oxfam nor LIFARS has been able to confirm that the threat actor has viewed or exfiltrated information from Oxfam's network, Oxfam understands that certain information contained on that part of its network that may have been accessed included human resources information, including names, addresses and social security numbers of its employees and their family members.

In response to the attack, Oxfam has, among other remedial measures, shut down Manage Engine and taken other appropriate action to disable unauthorized access to its system through Carbon Black, an endpoint security software designed to detect and prevent malicious files from attacking a system. Oxfam has also reported the attack to the United States Secret Service which is assisting in the forensic investigation into the attack.

Oxfam is not aware of, and has not received any reports or complaints of, the misuse of the personal information that was potentially accessed by the threat actor. That said, Oxfam recognizes that while it is unknown, based upon the forensic investigation that has been undertaken, whether the threat actor in fact accessed any human resources information on its network, there is the potential that such information may have been accessed. Oxfam will accordingly notify those individuals whose information may have been the subject of the unauthorized access and will advise those residents that steps should be taken to be alert to signs of any misuse of their personal information. These individuals will also be advised how to request a security freeze and the ability to obtain credit reports from any of the credit reporting agencies, and to remain vigilant by reviewing account statements and monitoring free credit reports. Oxfam will offer each person complimentary credit monitoring services for a period of two years. Oxfam expects to provide written notice to the potentially affected individuals within a week. A sample notification letter that Oxfam will send to the affected individuals is enclosed herewith.

Oxfam will, as noted above, continue to investigate this incident with the assistance of its retained forensic consultant, will monitor any inquiries from the persons potentially impacted, and will advise your office if any new significant information is learned.

We are, of course, available to discuss this matter with you, if you wish.

Very truly yours,



Christian W. Habersaat

Enclosure



[Date]

[Individual Name]

[Street Address]

[City/State/Postal Code]

Dear [Individual Name]:

We are writing to notify you of an incident that may have impacted the security of your personal information. We are providing you with information regarding the incident, steps we have taken since discovering the incident, and what you can do to protect identity theft and fraud.

### **What Happened**

On April 1, 2020, Oxfam learned of a cyber-security attack involving its network through which an unauthorized party potentially accessed certain personal information, including yours.

### **What Information Was Involved**

While Oxfam has not been able to confirm that the unauthorized party viewed your personal information, the information potentially accessed included names, addresses and social security numbers of Oxfam's employees.

### **What Oxfam Is Doing To Address This Situation**

Oxfam takes the security and confidentiality of the personal information entrusted to us very seriously. While Oxfam is not aware of and has not received any reports of the access or misuse of your personal information, it has taken the appropriate steps to ensure that your sensitive information has been secured. Oxfam is also conducting a thorough investigation into any unauthorized access of your personal information that may have occurred.

As a result of the potential unauthorized access of personal information, Oxfam will provide you, if you wish, with access to identity monitoring services provided by *InfoArmor*, an Allstate Company, at no charge for two years.

### **How To Enroll For The Free Services**

You will need to activate an account online by visiting [www.privacyarmor.com/oxfam](http://www.privacyarmor.com/oxfam) and clicking "Enroll Now" or by calling 1-800-789-2720 before May 29, 2020.

We have arranged a dedicated call center run by a third party, InfoArmor, to assist with questions about how to protect your identity following this incident. You may call InfoArmor at 1-800-789-2720, or e-mail at [ClientServices@InfoArmor.com](mailto:ClientServices@InfoArmor.com) who has a team of Privacy Advocates available 24/7.



[Individual Name]

[Date]

Page 2

---

### **What You Can Do To Address This Situation**

You may consider placing a security freeze on your credit report. A security freeze prohibits a credit-reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must contact each of the three major consumer reporting agencies: Equifax ([www.equifax.com](http://www.equifax.com)); Experian ([www.experian.com](http://www.experian.com)); and TransUnion ([www.transunion.com](http://www.transunion.com)):

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348  
800-685-1111  
[www.equifax.com/personal/credit-report-services/credit-freeze](http://www.equifax.com/personal/credit-report-services/credit-freeze)

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013  
888-397-3742  
[www.Experian.com/freeze/center/html](http://www.Experian.com/freeze/center/html).

Trans Union  
P.O. Box 160  
Woodlyn, PA 19094  
888-909-8872  
[www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

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.

[Individual Name]

[Date]

Page 3

---

The credit reporting agencies have one (1) business day after receiving your request by telephone or secure electronic means or three (3) business days after receiving your request by mail to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by a secure electronic means or mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one (1) hour after receiving your request by telephone or secure electronic means or three (3) business days after receiving your request by mail to lift the security freeze for those identified entities or for the specified period of time.

Although Oxfam is not aware of any reports of the access or misuse of your personal information we suggest that you should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect fraud, be sure to report it immediately to your financial institutions. In addition, you may contact the Federal Trade Commission ("FTC"), law enforcement or the attorney general's office to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at [identitytheft.gov](http://identitytheft.gov), or call the FTC, at (877) IDTHEFT (877-438-4338) or write to Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, [www.oag.state.md.us/idtheft](http://www.oag.state.md.us/idtheft), [idtheft@oag.statemd.us](mailto:idtheft@oag.statemd.us), or by calling 410-576-6491.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), or by calling 877-566-7226 or (919) 716-6000.

For Oregon residents, the Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us](http://www.doj.state.or.us) or by calling 877-877-9392

For Rhode Island residents, the Attorney General can be contacted at Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), or by calling 401-274-4400

### **For More Information**

At Oxfam we take our responsibilities to protect your personal information very seriously. We

[Individual Name]

[Date]

Page 4

are deeply disturbed by this situation and apologize for any inconvenience it may cause. If you have any questions or need further information regarding this incident, you may contact William Sablove in HR ([william.sablove@Oxfam.org](mailto:william.sablove@Oxfam.org)). Please recognize however that at this time we are unable to provide you with specific information as to the nature of the possible unauthorized access to your personal information.

Sincerely,

Angie Castera  
VP, People, Culture, and Global HR

OXFAM AMERICA  
226 CAUSEWAY STREET, 5TH FLOOR BOSTON, MA 02114-2206 USA  
TEL +1 (800) 776 9326 FAX +1 (617) 728 2594 [www.oxfamamerica.org](http://www.oxfamamerica.org)

STATE OF NEW YORK  
DEPT OF JUSTICE  
2020 APR 20 PM 1:31