



DLA Piper LLP (US)
The Marbury Building
6225 Smith Avenue
Baltimore, Maryland 21209-3600,
UNITED STATES OF AMERICA
www.dlapiper.com

Benjamin D. Schuman, Esq.

William W. Reichart III, Esq.

March 17, 2023

VIA E-Mail

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202
E-mail: idtheft@oag.state.md.us

Re: International Rescue Committee, Inc. – Incident Notification

Dear Sir or Madam:

We represent International Rescue Committee, Inc. (“IRC”), a global humanitarian aid, relief, and development nongovernmental organization located at 122 East 42nd Street, New York, New York, and are writing to notify your office of an incident that may affect the security of certain personal information relating to eighty-six (86) Maryland residents. This notice will be supplemented with any new material and significant facts uncovered by IRC subsequent to the submission of this notice. IRC’s reasonable and diligent investigation is on-going. By providing this notice, IRC does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about November 23, 2022, IRC learned that a now-former employee who was on administrative leave due to investigation of an unrelated incident downloaded certain files containing personal information of IRC’s clients. While the now-former employee previously had access to these files as part of their legitimate job duties, at the time of the incident the employee was prohibited from using the files under IRC’s internal policies as a result of his administrative leave status.

Upon learning of the incident on or about November 23, 2022, IRC quickly acted to terminate the employee’s access to all of IRC’s systems, including all personal information maintained by IRC. IRC also immediately launched an investigation to determine the nature and scope of the personal information downloaded by the employee. That investigation required careful manual analysis of files to determine when they were downloaded and the information contained in those files, as the employee previously had access and properly used them for his work on behalf of IRC and its



March 17, 2023

Page Two

clients. Through its investigation, IRC has determined that between October 27, 2022 and November 22, 2022, the now-former employee downloaded a limited number of files maintained by IRC for the provision of services to its clients including copies of public benefits applications, referral forms, and other documents maintained by IRC to assist clients. Those documents contain personal information including names, dates of birth, alien registration numbers, and social security numbers of IRC clients and/or their children. IRC then undertook another rigorous analysis to confirm which individuals were impacted. This review was recently completed.

Notice to Maryland Residents

Promptly following the date of this letter, IRC will provide written notice of this incident to 86 Maryland residents. Written notice is being provided in substantially the same form as the letter attached hereto as **Exhibit A**.¹

Other Steps Taken and To Be Taken

Upon discovering the event, IRC moved quickly to investigate and respond to the incident. IRC immediately responded by taking measures to prevent further unauthorized access of personal information by the now-former employee and by launching full investigation. IRC has been working diligently to provide its clients with an accurate and complete notice of the incident as quickly as possible.

As part of the ongoing commitment to the privacy and security of information in our care, IRC is conducting a full review of its internal systems, policies, and procedures relating to data protection and security. IRC is implementing enhanced measures, protocols, and employee training programs to better prevent future incidents, including concerning the management of employee access to personal information of IRC's clients. IRC is also working to implement additional safeguards and training to its employees to prevent similar incidents in the future.

Additionally, IRC is providing impacted individuals with guidance on how to better protect against identity theft and fraud. IRC is 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

¹ The written notice IRC intends to provide to the impacted Maryland residents will include certain information that is being translated into the native language of the impacted resident. Specifically, as noted in Exhibit A, IRC is translating a portion of the written notice into eleven different languages. The written notices will issue promptly after the translations have been completed and verified.



March 17, 2023

Page Three

reports, and encouragement to contact the Office of the Attorney General and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact the undersigned at (410) 580-4022.

Best Regards,

/s/ Benjamin D. Schuman

Benjamin D. Schuman

/s/ William W. Reichart III

William W. Reichart III

Enc.: Sample Notification Letter

EXHIBIT A



International Rescue Committee

122 East 42ND Street
New York, NY 10168-1289

Rescue.org

{Name of impacted individual}
{Address Line 1}
{Address Line 2}

Dear {Name of impacted individual}:

International Rescue Committee, Inc. (“IRC”) is writing to notify you of a recent incident that may affect the security of some of your personal information and/or personal information of your child. We take the privacy and security of your information very seriously. This notice provides additional information about the incident, our response, and the resources available to help protect your information from possible misuse, should you feel it is appropriate to do so.

IRC is committed to safeguarding the privacy and security of its clients and sincerely regrets that this incident occurred. IRC takes this event very seriously and that is why we are writing to provide you with additional information. IRC will continue to be forthcoming with any relevant information as it is discovered.

{TO BE TRANSLATED INTO 11 LANGUAGES} If you have questions about this letter and need an interpreter, please call 212-551-3020 and leave a message with your name, phone number, and preferred language. IRC will return your call with an interpreter.

What Happened?

IRC recently learned that a now-former employee accessed and downloaded certain personal information of IRC’s clients during a time when the employee was not authorized to do so. Specifically, between October 27, 2022 and November 22, 2022, the now-former employee downloaded certain files maintained by IRC for the provision of services to its clients including Department of Social Services Applications and other documents containing client names, dates of birth, alien registration numbers, and in some instances social security numbers. While the now-former employee previously had access to these files as part of their job responsibilities, at the time of the incident the employee was on administrative leave pending investigation for an unrelated incident. The employee is no longer employed with IRC.

IRC initially became aware of potential unauthorized access by the now-former employee on November 23, 2022. Upon learning of the incident on November 23, 2022, IRC quickly acted to terminate the employee’s access to all of IRC’s systems, including all personal information maintained by IRC. IRC also immediately launched an investigation to determine the nature and

scope of the personal information downloaded by the employee. That investigation required careful manual analysis of files to determine when they were downloaded and the information contained in those files, as the employee previously had access and properly used them for his work on behalf of IRC and its clients. Through the investigation, IRC determined that the employee downloaded a limited number of documents including copies of public benefits applications, referral forms, and other documents maintained by IRC to assist clients. Those documents contain personal information including names, dates of birth, alien registration numbers, and social security numbers of IRC clients and/or their children. IRC then undertook another rigorous analysis to confirm which individuals were impacted.

IRC conducted a thorough and comprehensive review of the downloaded files for sensitive information, and that review determined that certain information relating to you and/or your child was in the downloaded documents. If the information related to you, this letter has been addressed only to you. If the information related to you and your child, this letter has been addressed to both impacted individuals and directed to your care as the child's guardian.

What Information Was Involved?

Through our review, we determined that information relating to you and/or your child was downloaded including your full name, date of birth, alien registration number, and social security number (if you have one). **Please note, we are not aware of any misuse or attempted misuse of your personal information related to this event. We are sharing this information as part of our valued relationship with you and out of an abundance of caution.**

What Are We Doing?

We treat our responsibility to safeguard personal information in our possession as an utmost priority. As soon as IRC discovered this incident, we responded immediately by taking measures to prevent further unauthorized access of personal information by the now-former employee and by launching full investigation. IRC has been working diligently to provide you with an accurate and complete notice of the incident as quickly as possible.

As part of the ongoing commitment to the privacy and security of information in our care, we are conducting a full review of our internal systems, policies, and procedures relating to data protection and security. IRC is implementing enhanced measures, protocols, and employee training programs to better prevent future incidents, including concerning the management of employee access to personal information of IRC's clients.

In addition, through this notification, we are providing you with information below concerning what you can do to further protect your personal information.

What You Can Do

To date, we are not aware of any misuse of your information or the information of your child as a result of this incident. Out of an abundance of caution, however, we offer some suggestions you may consider for protecting your personal information or that of your child from potential misuse.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may receive copies of your free credit reports from the three major credit bureaus including Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus at the information listed below for credit reports. If your child's information was impacted by this incident, you may also contact the three major credit reporting bureaus to see if your child as a credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one-year alert is placed on a consumer's credit file. A fraud alert tells creditors to contact you personally before they open any new accounts. If your child has a credit report, you may also place a fraud alert on your child's credit file. To place a fraud alert, contact any one of the three major credit reporting bureaus at the information listed below for fraud alerts. As soon as one credit bureau confirms a fraud alert, they will notify the others.

Consumers may also place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit 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 credit 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. To request a credit freeze, you may contact the three major credit reporting bureaus at the information listed below for credit freezes. Please note, to request a credit freeze you will need to provide the following information: (1) full name, (2) social security number, (3) date of birth, (4) address for the prior two to five years, (5) proof of current address, (6) a legible copy of a government-issued identification card, and (7) a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Contact Information for Credit Reporting Bureaus

	<i>Equifax</i>	<i>Experian</i>	<i>TransUnion LLC</i>
website	https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
phone	1-888-298-0045	1-888-397-3742	1-833-395-6938
fraud alert	Equifax Fraud Alert, P.O. Box 105069, Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
credit freeze	Equifax Credit Freeze, P.O. Box 105788, Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

You may also obtain information about avoiding identify theft from the Maryland Attorney General at: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, Maryland 21202, (888) 743-0023 (toll free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps to take to protect your personal information by contacting the Federal Trade Commission at 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338).

For More Information

If you have any questions regarding this incident, or if you desire any further information or assistance, please call IRC at 212-551-3020, Monday through Friday from 9:00 am – 5:00 pm Eastern Time, excluding major U.S. holidays. IRC's Maryland office is located at 1900 N. Howard Street, Suite 200, Baltimore, Maryland 21218.

IRC takes your trust in us, and this matter, very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

International Rescue Committee, Inc.