Save the Children®

Office of the Attorney General
Attn: Security Breach Notification
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

August 14, 2020

To Whom It May Concern:

We are writing to inform you that Save the Children was notified on July 16 of a cyberattack by Blackbaud, a company that provides software tools and management resources for nonprofits across the world, including Save the Children.

What Happened
We understand from Blackbaud that the incident began in February, when the hacker gained access to Blackbaud's system, and continued until May 2020, when Blackbaud discovered the hacker was attempting to carry out a ransomware attack. At that time, Blackbaud worked with their own security teams, an external forensics firm and federal law enforcement to expel the attacker from their system. Unfortunately, the hacker was able to make a copy of data on the system, and Blackbaud subsequently paid a ransom to the hacker to have them delete the data. Additional information on the incident is **available on Blackbaud's website.**

What Information Was Involved
Although Save the Children had recently migrated off of Blackbaud's hosting solution, Blackbaud's system still housed a backup of Save the Children's supporter database. The database included names, contact information, details of our supporters' relationship with Save the Children (e.g. event participation and giving history), some biographic details (e.g. date of birth), and additional information, although not all of these details were present in every record. In addition, Save the Children believes that in some instances the information included the image of scanned checks provided by supporters in the course of a donation. And in some instances, EFT details of supporters' donation were involved which were encrypted using AES-256 encryption; Save the Children is not aware of any evidence that any key allowing decryption of such details was compromised in the incident. The number of Washington residents involved whose data is subject Washington's state notification law is 47,465.

What we are doing
Since July 16, we have been in contact with Blackbaud to obtain more

Save the Children®

information about this incident. Although Blackbaud believes that the risk to individuals whose data was stolen is very low, they have put in place dark web monitoring intended to detect trafficking of any of the copied data. In the meantime, we have removed our data from Blackbaud's servers, and we will continue to take steps to protect our supporters' data, both internally and with all of our third-party vendors. Although we have no reason to believe that any individual has suffered or is at significant risk of suffering any harm as a result of this incident, or that that this incident presents a high risk to the rights and freedoms of individuals whose information was involved, we anticipate providing written notice, conforming to the statutory requirements, to potentially-affected individuals whose addresses have been found in the affected data by first-class mail on or about August 20, 2020. For the small number of individuals whose scanned checks were involved, we are providing 12 months of credit monitoring services free of charge. Forms of those individual notices are attached. In addition, we have provided an overview of the situation to a substantial number of supporters by email and posted a press release on our website concerning the incident. We continue to assess whether further notification efforts are appropriate.

Sincerely Yours,

DocuSigned by:
Brian M. White
9CA0120EF7F14D6...

Brian M. White
Deputy General Counsel and
Chief Compliance Officer

501 Kings Highway East
Suite 400
Fairfield, CT 06825
1-800 Save the Children
www.SavetheChildren.org

Save the Children®

Date

First Name Middle Name Last Name
Street Address
City, State Zip

Dear Prefix Last Name,

We are writing to inform you that Save the Children was notified on July 16 of a cyberattack at one of our vendors, Blackbaud. Blackbaud provides software tools and management resources for nonprofits across the world, including Save the Children. Save the Children takes cyber security and the protection of your information very seriously, therefore we are contacting you to explain the incident.

What Happened
We understand from Blackbaud that the incident began in February, when the hacker gained access to Blackbaud's system, and continued until May 2020, when Blackbaud discovered the breach. At that time, Blackbaud worked with their own security teams, an external forensics firm and federal law enforcement to expel the attacker from their system. However, the hacker was still able to copy data from Blackbaud's server. Blackbaud subsequently paid a ransom to the hacker to have them delete the data. Unfortunately, Save the Children was one of a number of organizations impacted by this security breach. Additional information on the incident is available on Blackbaud's website (*https://www.blackbaud.com/securityincident*).

What Information Was Involved
Blackbaud's system housed some of Save the Children's supporter information. For you, this data included: [*placeholder for recipient's data*] **Importantly, the following information is either not collected by Save the Children or is not stored in the database at issue, and therefore was not involved: payment card numbers, account passwords or PINs, social security numbers, and government identification or passport details or numbers.**

What We Are Doing
Save the Children places a high level of regard on security and protecting our donor information. Since July 16, we have been in contact with Blackbaud to obtain more information about this incident. Although Blackbaud believes the risk to individuals whose data was stolen is very low, they have put in place dark web monitoring intended to detect trafficking of any of the copied data.

Supporters like you trust us with their information, and we do not take this lightly. We have removed our data off Blackbaud's servers, and we will continue to take steps to protect your data, both internally and with all of our third-party vendors.

What You Can Do
Although we have no information indicating that any of the information impacted by this incident has been misused, Save the Children encourages you to remain vigilant against identity theft and "phishing" scams. In particular, please pay close attention to any

communications that appear to be from Save the Children, and if you have any questions about them, please contact us at the phone number below.

You may further protect yourself by monitoring free credit reports available from the major credit reporting agencies, for any indication of unexpected activity, and by instituting fraud alerts and security freezes on your credit report profiles [over the next 12 to 24 months]. You may also ask for certain information or assistance from state or federal law enforcement. These measures are discussed further in the Appendix to this letter.

For More Information
If you have any immediate concerns or questions, please contact 1-877-277-3947.

Thank you for your partnership and support.

Very truly yours,
Eric Howell
Executive Vice President & Chief Operating Officer

Save the Children®

Appendix: Resources for Supporters Whose Data Could Have Been Exposed

I. There may be additional ways to protect yourself:

A. Measures that you can take to protect yourself with regard to consumer credit reporting bureaus:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

Fraud Alert. When you place a "fraud alert" on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other three bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A "security freeze" or "credit freeze" goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

- prevent you from getting your free annual credit report;
- keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance;
- prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Save the Children®

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and other personal information. Credit reporting agencies are required to place or remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies, the Federal Trade Commission, and various state authorities. You may obtain additional information from these resources about preventing or remedying identity theft, including by setting up fraud alerts or security freezes and by reviewing your credit report. The contact information of those agencies is provided below:

	Fraud Alerts	*Security Freezes*	*Credit Reports*
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069 888-836-6351 (automated service line) 800-525-6285 (customer care agents) https://my.equifax.com/consumer-registration/UCSC/#/personal-info	Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 888-298-0045 (customer care agents) https://my.equifax.com/consumer-registration/UCSC/#/personal-info	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374-0241 866-349-5191 (automated service line) https://www.annualcreditreport.com/index.action
Experian	Experian P.O. Box 4500 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 (regular mail) Experian 711 Experian Parkway Allen, TX 75013 (overnight mail) 1-888-397-3742 https://www.experian.com/freeze/center.html	Experian P.O. Box 4500 Allen, TX 75013 1-888-397-3742 https://www.annualcreditreport.com/index.action

TransUnion	TransUnion Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016 888-909-8872 https://fraud.transunion.com	TransUnion LLC P.O. Box 2000 Chester, PA 19016 888-909-8872 https://freeze.transunion.com/	Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281 800-888-4213 https://www.annualcreditreport.com/index.action

B. Information and assistance that you can obtain from federal and state law enforcement and consumer protection agencies:

If you believe that you may be the victim of identity theft or have reason to believe your personal information was misused you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC by mail, by phone, or online at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

C. Protections of the Federal Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary or your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room*

130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, as of September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. *See www.ftc.gov/credit for additional information.*

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. *See www.ftc.gov/credit for an explanation of dispute procedures.*

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable

information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit.*

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).*

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active duty military personnel have additional rights. *For more information, visit www.ftc.gov/credit.*

Source: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

II. If you are a resident of certain US states, you may have additional resources available to you:

A. Connecticut

If you are a resident of Connecticut, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, (860) 808-5318, www.ct.gov/ag.

B. Iowa

If you are a resident of Iowa, you may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You

can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov/.

C. Maryland

If you are a resident of Maryland, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or by calling (410) 576-6491. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General at: Identity Theft Unit, Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

D. Massachusetts

If you are a resident of Massachusetts, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You also have the right to request a security freeze. And, you may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, (617) 727-8400, www.mass.gov/ago/contact-us.html.

E. New York

If you are a resident of New York, you may contact and obtain information about security breach response and identity theft prevention and protection from the following New York state agencies: (i) New York Attorney General Consumer Frauds & Protection Bureau, 120 Broadway, 3rd Floor, New York, NY 10271, (800) 771-7755, www.ag.ny.gov; (ii) New York Department of State Division of Consumer Protection, 99 Washington Avenue, Suite 650, Albany, NY 12231, (800) 697-1220, www.dos.ny.gov.

F. North Carolina

If you are a resident of North Carolina, you may contact and obtain information from the state attorney general at: Office of the Attorney General, 9001 Mail Service Center Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov.

G. Oregon

If you are a resident of Oregon, you may contact and obtain information from the state attorney general at: Office of the Attorney General, 1162 Court Street NE, Salem, OR 97301, (503) 378-6002, www.doj.state.or.us/oregon-department-of-justice/office-of-the-attorney-general/attorney-general-ellen-f-rosenblum/.

H. Rhode Island

If you are a resident of Rhode Island, you may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South MainStreet, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400. Additionally, pursuant to Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

I. Washington D.C.

If you are a resident of Washington D.C., you may contact and obtain information from the state attorney general at: Office of the Attorney General for the District of Columbia, 441 4th St NW #1100, Washington, DC 20001, (202) 727-3400, www.oag.dc.gov/.

J. West Virginia

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. You also have a right to place a security freeze on your credit report.

Save the Children®

Date

First Name Middle Name Last Name
Street Address
City, State Zip

Dear Prefix Last Name,

We are writing to inform you that Save the Children was notified on July 16 of a cyberattack at one of our vendors, Blackbaud. Blackbaud provides software tools and management resources for nonprofits across the world, including Save the Children. Save the Children takes cyber security and the protection of your information very seriously, therefore we are contacting you to explain the incident.

What Happened
We understand from Blackbaud that the incident began in February, when the hacker gained access to Blackbaud's system, and continued until May 2020, when Blackbaud discovered the breach. At that time, Blackbaud worked with their own security teams, an external forensics firm and federal law enforcement to expel the attacker from their system. However, the hacker was still able to copy data from Blackbaud's server. Blackbaud subsequently paid a ransom to the hacker to have them delete the data. Unfortunately, Save the Children was one of a number of organizations impacted by this security breach. Additional information on the incident is available on Blackbaud's website (*https://www.blackbaud.com/securityincident*).

What Information Was Involved
Blackbaud's system housed some of Save the Children's supporter information. For you, this data included: [*placeholder for recipient's data*] In addition, we believe that a scanned copy of a check that you had provided to Save the Children was attached to your record. **Importantly, the following information is either not collected by Save the Children or is not stored in the database at issue, and therefore was not involved: payment card numbers, account passwords or PINs, social security numbers, and government identification or passport details or numbers.**

What We Are Doing
Save the Children places a high level of regard on security and protecting our donor information. Since July 16, we have been in contact with Blackbaud to obtain more information about this incident. Although Blackbaud believes the risk to individuals whose data was stolen is very low, they have put in place dark web monitoring intended to detect trafficking of any of the copied data.

Supporters like you trust us with their information, and we do not take this lightly. We have removed our data off Blackbaud's servers, and we will continue to take steps to protect your data, both internally and with all of our third-party vendors.

What You Can Do
Although we have no information indicating that any of the information impacted by this incident has been misused, Save the Children encourages you to remain vigilant against

identity theft and “phishing” scams. In particular, please pay close attention to any communications that appear to be from Save the Children, and if you have any questions about them, please contact us at the phone number below.

You may further protect yourself by monitoring free credit reports available from the major credit reporting agencies, for any indication of unexpected activity, and by instituting fraud alerts and security freezes on your credit report profiles [over the next 12 to 24 months]. You may also ask for certain information or assistance from state or federal law enforcement. These measures are discussed further in the Appendix to this letter.

Further, although Save the Children has no reason to believe that the scan of your check may be misused, it has made credit monitoring services, identity theft restoration services, and identity theft insurance available to you at no charge for 12 months. Details of how to activate these services is included in Section III of the Appendix to this letter.

For More Information
If you have any immediate concerns or questions, please contact 1-877-277-3947.

Thank you for your partnership and support.

Very truly yours,
Eric Howell
Executive Vice President & Chief Operating Officer

Save the Children®

Appendix: Resources for Supporters Whose Data Could Have Been Exposed

I. There may be additional ways to protect yourself:

A. Measures that you can take to protect yourself with regard to consumer credit reporting bureaus:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

Fraud Alert. When you place a "fraud alert" on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other three bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A "security freeze" or "credit freeze" goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

- prevent you from getting your free annual credit report;
- keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance;
- prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and other personal information. Credit reporting agencies are required to place or remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies, the Federal Trade Commission, and various state authorities. You may obtain additional information from these resources about preventing or remedying identity theft, including by setting up fraud alerts or security freezes and by reviewing your credit report. The contact information of those agencies is provided below:

	Fraud Alerts	*Security Freezes*	*Credit Reports*
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069 888-836-6351 (automated service line) 800-525-6285 (customer care agents) https://my.equifax.com/consumer-registration/UCSC/#/personal-info	Equifax Information Services LLC P.O. Box 105788 Atlanta, GA 30348-5788 888-298-0045 (customer care agents) https://my.equifax.com/consumer-registration/UCSC/#/personal-info	Equifax Information Services LLC P.O. Box 740241 Atlanta, GA 30374-0241 866-349-5191 (automated service line) https://www.annualcreditreport.com/index.action
Experian	Experian P.O. Box 4500 Allen, TX 75013 1-888-397-3742 https://www.experian.com/fraud/center.html	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 (regular mail) Experian 711 Experian Parkway Allen, TX 75013 (overnight mail) 1-888-397-3742 https://www.experian.com/freeze/center.html	Experian P.O. Box 4500 Allen, TX 75013 1-888-397-3742 https://www.annualcreditreport.com/index.action

TransUnion	TransUnion Fraud Victim Assistance Department P.O. Box 2000 Chester, PA 19016 888-909-8872 https://fraud.transunion.com	TransUnion LLC P.O. Box 2000 Chester, PA 19016 888-909-8872 https://freeze.transunion.com/	Annual Credit Report Request Service P.O. Box 105281 Atlanta, GA 30348-5281 800-888-4213 https://www.annualcreditreport.com/index.action

B. Information and assistance that you can obtain from federal and state law enforcement and consumer protection agencies:

If you believe that you may be the victim of identity theft or have reason to believe your personal information was misused you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC by mail, by phone, or online at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

C. Protections of the Federal Fair Credit Reporting Act

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary or your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer*

Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, as of September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. *See www.ftc.gov/credit for additional information.*

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. *See www.ftc.gov/credit for an explanation of dispute procedures.*

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable

information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit.*

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).*

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active duty military personnel have additional rights. *For more information, visit www.ftc.gov/credit.*

Source: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

II. If you are a resident of certain US states, you may have additional resources available to you:

A. Connecticut

If you are a resident of Connecticut, you may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, (860) 808-5318, www.ct.gov/ag.

Save the Children®

B. Iowa

If you are a resident of Iowa, you may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. You can contact the Iowa Attorney General at: Office of the Attorney General, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov/.

C. Maryland

If you are a resident of Maryland, you may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or by calling (410) 576-6491. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General at: Identity Theft Unit, Office of the Attorney General, 200 St. Paul Place, 25th Floor, Baltimore, MD 21202, (888) 743-0023, www.oag.state.md.us.

D. Massachusetts

If you are a resident of Massachusetts, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. You also have the right to request a security freeze. And, you may contact and obtain information from your state attorney general at: Office of the Massachusetts Attorney General, One Ashburton Place, Boston, MA 02108, (617) 727-8400, www.mass.gov/ago/contact-us.html.

E. New York

If you are a resident of New York, you may contact and obtain information about security breach response and identity theft prevention and protection from the following New York state agencies: (i) New York Attorney General Consumer Frauds & Protection Bureau, 120 Broadway, 3rd Floor, New York, NY 10271, (800) 771-7755, www.ag.ny.gov; (ii) New York Department of State Division of Consumer Protection, 99 Washington Avenue, Suite 650, Albany, NY 12231, (800) 697-1220, www.dos.ny.gov.

F. North Carolina

If you are a resident of North Carolina, you may contact and obtain information from the state attorney general at: Office of the Attorney General, 9001 Mail Service Center Raleigh, NC 27699-9001, (919) 716-6400, www.ncdoj.gov.

Save the Children®

G. Oregon

If you are a resident of Oregon, you may contact and obtain information from the state attorney general at: Office of the Attorney General, 1162 Court Street NE, Salem, OR 97301, (503) 378-6002, www.doj.state.or.us/oregon-department-of-justice/office-of-the-attorney-general/attorney-general-ellen-f-rosenblum/.

H. Rhode Island

If you are a resident of Rhode Island, you may contact and obtain information from your state attorney general at: Rhode Island Attorney General's Office, 150 South MainStreet, Providence, RI 02903, www.riag.ri.gov, (401) 274-4400. Additionally, pursuant to Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

I. Washington D.C.

If you are a resident of Washington D.C., you may contact and obtain information from the state attorney general at: Office of the Attorney General for the District of Columbia, 441 4th St NW #1100, Washington, DC 20001, (202) 727-3400, www.oag.dc.gov/.

J. West Virginia

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. You also have a right to place a security freeze on your credit report.

III. Save the Children will provide you with credit monitoring and identity restoration services:

To help protect your identity, Save the Children is also offering a complimentary one-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by: November 7, 2020 (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your activation code: [code]

Save the Children®

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by November 7, 2020. Be prepared to provide engagement number DB21930 as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 12-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** 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. Offline members will be eligible to call for additional reports quarterly after enrolling.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files 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.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers. 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 1-877-288-8057. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year 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. You will also find self-help tips and information about identity protection at this site.