



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

RECEIVED  
JUL 06 2021

CONSUMER PROTECTION  
5133 Harding Pike, B-10, #310  
Nashville, TN 37205-2891

Alexandria N. Murphy  
Office: (267) 930-1345  
Fax: (267) 930-4771  
Email: amurphy@mullen.law

June 30, 2021

**VIA U.S. MAIL**

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 Safer Foundation, located at 571 W. Jackson Blvd., Chicago IL 60661, and are writing to notify your office of an incident that may affect the privacy of some personal information relating to one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned after its submission. By providing this notice, Safer Foundation 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**

Safer Foundation experienced a data security event that impacted computer system operations and caused a temporary disruption to certain client services. Safer Foundation immediately launched an investigation to determine the nature and scope of the incident. As part of its investigation into the root cause of the incident, Safer Foundation's email system was reviewed for evidence of suspicious activity. Through that review, Safer Foundation confirmed that two employee email accounts, which could have contained sensitive information, had been subject to unauthorized access intermittently between July 24 and August 31, 2020. However, the investigation was unable to determine which, if any, emails and attachments in these accounts were viewed by the unauthorized actor. Therefore, Safer Foundation conducted a thorough review of the potentially at-risk contents of the accounts to determine whether they contained any sensitive information. When Safer Foundation received the results of this review, it determined that certain sensitive information was accessible in the email accounts during the period of unauthorized access. As

such, Safer Foundation undertook efforts to locate address information for potentially impacted individuals and determine its relationship to those individuals in order to provide them with notice.

Safer Foundation cannot confirm if the unauthorized actor(s) accessed or viewed any specific information relating to individuals. However, Safer Foundation recently determined that the information present in one of the impacted accounts and therefore accessible at the time of the incident included the following data related to a New Hampshire resident: name and Social Security number.

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

On or about June 30, 2021, Safer Foundation began providing 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*.

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

Safer Foundation has taken steps to enhance the security of its systems, including resetting the affected employees' email account passwords. As part of its ongoing commitment to the privacy and security of information entrusted to it, Safer Foundation is providing enhanced training to employees regarding data privacy and information security best practices. Safer Foundation is also in the process of reviewing its existing policies and procedures to mitigate any risks associated with this event and to better prevent future events. Safer Foundation is providing potentially affected individuals access to complimentary credit monitoring services for one (1) year through Kroll.

Additionally, Safer Foundation is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Safer Foundation 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 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.

Office of the New Hampshire Attorney General  
June 30, 2021  
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) 930-1345.

Very truly yours,

A handwritten signature in cursive script, appearing to read "Alexandria N. Murphy".

Alexandria N. Murphy of  
MULLEN COUGHLIN LLC

ANM/eyl

# EXHIBIT A



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

**NOTICE OF <<b2b\_text\_1(SubjectLine)>>**

Dear <<MemberFirstName>> <<MemberLastName>>:

Safer Foundation is committed to protecting the privacy and security of the information entrusted to us. We are writing to inform you of a recent event that may impact some of your information. Although we are unaware of any actual or attempted misuse of your information, we are providing you with details about the event, steps we have taken in response, and resources available to help you better protect your information, should you feel it is appropriate to do so.

**What Happened?** We experienced a data security event that impacted computer system operations and caused a temporary disruption to our client services. We immediately launched an investigation to determine the nature and scope of the incident. As part of our investigation into the root cause of the incident, our email system was reviewed for evidence of suspicious activity. Through that review, we confirmed that two employee email accounts, which could have contained sensitive information, had been subject to unauthorized access intermittently between July 24 and August 31, 2020. However, the investigation was unable to determine which, if any, emails and attachments in these accounts were viewed by the unauthorized actor. Therefore, we conducted a thorough review of the potentially at-risk contents of the accounts to determine whether they contained any sensitive information. When we received the results of this review, we determined that certain sensitive information was accessible in the email accounts during the period of unauthorized access. As such, we undertook efforts to locate address information for potentially impacted individuals and determine our relationship to those individuals in order to provide this notice.

**What Information Was Involved?** We cannot confirm if the unauthorized actor(s) accessed or viewed any specific information relating to you. However, we recently determined that the information present in one of the impacted accounts and therefore accessible at the time of the incident included your <<b2b\_text\_2(Data elements)>>.

**What We Are Doing.** We have taken steps to enhance the security of our systems, including resetting the affected employees' email account passwords. As part of our ongoing commitment to the privacy and security of information in our care, we are providing enhanced training to employees regarding data privacy and information security best practices. We are in the process of reviewing our existing policies and procedures to mitigate any risks associated with this event and to better prevent future events.

Out of an abundance of caution, we are also providing you with 12 months of complimentary access to identity monitoring services through Kroll, along with guidance on how to better protect against the possibility of information misuse. We are covering the cost of these services, but due to privacy restrictions, you will need to complete the activation process yourself using the activation instructions provided in the enclosure to this letter.

***What You Can Do.*** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanations of benefits, as applicable, and by monitoring your free credit reports for suspicious activity and to detect errors. You can find out more about how to better protect against the potential misuse of information in the enclosed *Steps You Can Take to Help Protect Your Information*. There, you will also find more information about the identity monitoring services we are offering and how to activate.

***For More Information.*** We understand that you may have questions about this event that are not addressed in this letter. If you have additional questions, please call 1-???-???-????, 8:00 am to 5:30 pm Central Time Monday through Friday, excluding U.S. holidays. You may also write to us at: Safer Foundation, ATTN: Henrietta Mason, Vice President Human Resources & Organizational Development, 571 W. Jackson Blvd., Chicago IL 60661.

We apologize for any inconvenience this incident may cause you and remain committed to the privacy and security of information in our possession.

Sincerely,

*Henrietta Mason*

Henrietta Mason  
Vice President Human Resources & Organizational Development  
Safer Foundation

## Steps You Can Take to Help Protect Your Information

### **Activate 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 one year. 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 <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

*You have until **September 16, 2021** to activate your identity monitoring services.*

Membership Number: <<Member ID>>

You have been provided with access to the following services 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 will be able to help you determine if it is 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

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.

### **Monitor Your Accounts**

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. 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 directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 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 three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to 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. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);

2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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.); 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.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
<a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a>	<a href="https://www.experian.com/help/">https://www.experian.com/help/</a>	<a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a>
1-888-298-0045	1-888-397-3742	1-833-395-6938
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
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

#### **Additional Information**

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may 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 Maryland residents*, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and [www.oag.state.md.us](http://www.oag.state.md.us).

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).

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

2021 JUL -6 PM 12:01

STATE OF NY  
DEPT OF JUSTICE