MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 1, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent the American Cancer Society, Inc ("ACS") located at 250 Williams Street, Atlanta, Georgia 30303. We are writing to notify your office of an incident that may affect the security of certain personal information relating to forty-two (42) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, ACS 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

On or about, January 31, 2019, ACS discovered suspicious activity related to a small number of employee email accounts. ACS immediately launched an investigation and discovered that the organization was the victim of a recent sophisticated phishing attack. ACS immediately began changing user passwords resulting in an enterprise wide password change to prevent further unauthorized access to employee email accounts as a result of this event. Industry leading forensic experts were retained to assist with determining the nature and scope of the incident. The investigation determined that a small number of employee email accounts were accessed without authorization between January 8, 2019 and January 31, 2019. The investigation also determined that no other ACS platforms or systems were affected. Unfortunately, the investigation was not able to determine which emails, if any, were specifically accessed. Out of an abundance of caution, a review of the contents of the email accounts was undertaken to identify what information may have been accessible and who may be affected. It was determined that certain information related to certain individuals was accessible in the email accounts.

The information that was accessible within the accounts includes a combination of name and Social Security number.

Notice to New Hampshire Residents

On or about March 1, 2019, ACS began providing written notice of this incident to affected individuals, which includes forty-two (42) New Hampshire residents. 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

Upon discovering the event, ACS moved quickly to investigate and respond to the incident, assess the security of ACS' systems, and notify potentially affected individuals. ACS has security measures, policies, and procedures in place to protect information and ACS continues to review these measures as part of its ongoing commitment to the security of the information in its care. ACS is also working to continue to educate all staff and improve its cyber security practices to help prevent a phishing attack like this from occurring in the future.

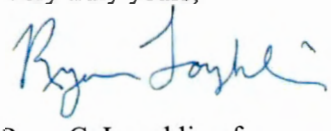
ACS is providing complimentary access to one year of credit monitoring, fraud consultation, and identity theft restoration services through Kroll Cyber Security, to individuals whose personal information was accessible within the employee email accounts. Additionally, ACS is also working to continue to educate all staff and improve our cyber security practices to help prevent a phishing attack like this from occurring in the future is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including 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.

ACS notified law enforcement of the event and is notifying all necessary state and federal regulators as well as the three major consumer reporting agencies.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL/ara
Enclosure

EXHIBIT A

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

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

Dear <<FirstName>> <<LastName>>,

We write to inform you of a recent event that could potentially affect the security of some of your personal information. While we are unaware of any actual or attempted misuse of your personal information, the American Cancer Society ("ACS") takes this incident very seriously and we are providing you with information and access to resources so that you can better protect your personal information, should you feel it is appropriate to do so.

What Happened? On or about, January 31, 2019, we discovered suspicious activity related to a small number of employee email accounts. We immediately launched an investigation and discovered that the organization was the victim of a recent sophisticated phishing attack. ACS immediately implemented an enterprise wide change of credentials to ensure the security of all ACS email accounts. Industry leading forensic experts were retained to assist with determining the nature and scope of the incident. The investigation determined that a small number of employee email accounts were accessed without authorization between January 8, 2019 and January 31, 2019. The investigation also determined that no other ACS platforms or systems were affected. Unfortunately, the investigation was not able to determine which emails, if any, were specifically accessed. Out of an abundance of caution, a review of the contents of the email accounts was undertaken to identify what information may have been accessible and who may be affected. It was determined that certain information related to you was accessible in the email accounts.

What Information Was Involved? Our investigation determined that the information related to you that was accessible in the emails included: <<ClientDef1(data elements)>><<ClientDef2(data elements)>>.

What We Are Doing. ACS is committed to protecting the confidentiality and security of all the information we hold in our care. We have security measures, policies, and procedures in place to protect this data and we continue to review these measures as part of our ongoing commitment to the security of the information in our care. We are reporting this incident to applicable state and federal regulators as well as to the individuals who may be affected by this incident. We are also providing you with information about this event and about the steps you can take to better protect against misuse of your personal information, should you feel it appropriate to do so.

As an added precaution, we are also offering you access to one year of credit monitoring and identity theft restoration services through Kroll Cyber Security at no cost to you. The cost of this service will be paid for by ACS. We encourage you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity theft protection services we are offering.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-877-481-6091 between 9 AM and 6:30 PM EDT Monday through Friday excluding major U.S. holidays.

Sincerely,

TB Phillips

Timothy Phillips
Chief Legal and Risk Officer

Steps You Can Take to Protect Against Identity Theft and Fraud

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 **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

You have until May 30, 2019 to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-877-481-6091. Additional information describing your services is included with this letter.

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 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:

Experian
PO Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

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:

Experian
P.O. Box 2002
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

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, 1-877-ID-THEFT (1-877-438-4338); 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 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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 violator. 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 29 Rhode Island residents impacted by this incident.

Kroll

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] 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.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. 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.