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

December 17, 2018

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:

Our firm represents Special Olympics Kentucky, 105 Lakeview Court, Frankfort, Kentucky 40601. We write to notify your office of an incident that may affect the privacy of certain personal information relating to two (2) New Hampshire residents. By providing this notice, Special Olympics Kentucky does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

On September 12, 2018, Special Olympics Kentucky became aware of suspicious activity in an employee's email account when the employee's email account was used to send out phishing emails. As a result of this activity, Special Olympics Kentucky immediately launched an investigation with the assistance of a leading forensic investigation firm to determine the full nature and scope of this activity. Through the investigation, it was determined on September 26, 2018 that an unauthorized actor obtained email login credentials for certain Special Olympics Kentucky employee email accounts, which resulted in unauthorized access to the employees' email accounts from April 17, 2018 – September 11, 2018. Special Olympics Kentucky took steps to change the employees' email credentials, and in the abundance of caution instituted a global password reset for all users on the Special Olympics Kentucky email system. The investigation was not able to determine what information, if any, was accessed or viewed by the unknown actor. Since the investigation was not able to determine what information, if any, was viewed, the contents of the accounts were reviewed through manual and programmatic processes to determine what information may have been accessible.

The investigation determined that the following information related to two (2) New Hampshire residents was present in the emails affected by this incident: name, Social Security number, and driver's license number.

Notice to New Hampshire Residents

Since discovering this incident, Special Olympics Kentucky has been working diligently to confirm the nature and scope of the event, determine which individuals may have been affected, and determine contact information for those individuals. On or around December 17, 2018, Special Olympics Kentucky began mailing written notice of this incident to potentially affected individuals, including two (2) 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 unusual activity in an employees' email, Special Olympics Kentucky immediately took steps to investigate and respond to the incident, including changing the affected users' email credentials, and implementing a global password reset on the Special Olympics Kentucky email system. Special Olympics Kentucky has been working diligently, with the assistance of third party forensic investigators, to ensure the security of its email environment, determine the full nature and scope of the event, and identify potentially affected individuals. While Special Olympics Kentucky has measures in place to protect information in its systems, it is exploring the implementation of additional safeguards including multi-factor authentication processes to protect the security of information.

Additionally, while the investigation has found no evidence of actual or attempted misuse of personal information potentially affected by this event, in an abundance of caution, Special Olympics Kentucky is providing potentially impacted individuals with notice of this event and with complimentary access to credit monitoring and identity theft protection services for 12 months through AllClear ID. Special Olympics Kentucky is also providing potentially 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 explanation of benefits form 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. Special Olympics Kentucky will also be providing notice of this event to other state regulators as required by law.

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/AMS
Enclosure

EXHIBIT A

Special Olympics Kentucky
Processing Center • P.O. BOX 141578 • Austin, TX 78714

00001 R834601
JOHN Q. SAMPLE
1234 MAIN STREET
ANYTOWN US 12345-6789

December 17, 2018

Dear John Sample:

Special Olympics Kentucky writes to inform you of a recent event that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused, we are making you aware of the event, so you may take steps to better protect against the possibility of identity theft or fraud, should you feel it necessary to do so.

What Happened? On September 12, 2018, Special Olympics Kentucky became aware of suspicious activity in an employee's email account when the employee's email account was used to send out phishing emails. As a result of this activity, Special Olympics Kentucky immediately launched an investigation with the assistance of a leading forensic investigation firm to determine the full nature and scope of this activity. Through the investigation, it was determined on September 26, 2018 that an unauthorized actor obtained email login credentials for certain Special Olympics Kentucky employee email accounts, which resulted in unauthorized access to the employees' email accounts from April 17, 2018 – September 11, 2018. Special Olympics Kentucky took steps to change the employees' email credentials, and in the abundance of caution instituted a global password reset for all users on the Special Olympics Kentucky email system. The investigation was not able to determine what information, if any, was accessed or viewed by the unknown actor.

Since the investigation was not able to determine what, if any, information was viewed, the contents of the accounts were reviewed through manual and programmatic processes to determine what sensitive data may have been accessible. On October 19, 2018, after the completion of the review, it was determined that the accounts may contain certain information related to you.

What Information Was Involved? While we currently have no evidence that your information was subject to actual or attempted misuse, we have confirmed that your name and Social Security number were contained within the affected employee email accounts.

What We Are Doing. The confidentiality, privacy, and security of information in our care is one of our highest priorities. Upon learning of this incident, we took steps to secure the affected email accounts and to find out what happened. As part of our ongoing commitment to the security of the information in our care, we are reviewing our existing policies and procedures, and exploring the implementation of multi-factor authentication protocols for our email systems.

01-03-1

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-263-2174 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a $1 million identity theft insurance policy. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-263-2174 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

What You Can Do. You may review the enclosed "*Steps You Can Take to Prevent Identity Theft and Fraud*" for information on remaining vigilant and protecting against incidents of identity theft and fraud. You may also enroll to receive the free identity theft protection and identity repair services described above.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, you can call our dedicated assistance line at 1-855-263-2174, Monday through Saturday from 8:00 a.m. to 8:00 p.m. Central Time.

Special Olympics Kentucky takes the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,

Trish Mazzoni

Trish Mazzoni
President/CEO
Special Olympics Kentucky

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

In addition to enrolling to receive the complimentary monitoring services, 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	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	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.

AllClear Identity Repair Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 12 months of coverage with no enrollment required.
- No cost to you — ever. AllClear Identity Repair is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Identity Repair is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 12 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events (each, an "Event") that were discovered prior to your Coverage Period are not covered by AllClear Identity Repair services.

Eligibility Requirements
To be eligible for Services under AllClear Identity Repair coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Identity Repair services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period;
- Provide proof of eligibility for AllClear Identity Repair by providing the redemption code on the notification letter you received from the sponsor Company;
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require; and
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft.

Coverage under AllClear Identity Repair Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge, or
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation");
- Incurred by you from an Event that did not occur during your coverage period; or
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Identity Repair coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity.
- AllClear ID is not an insurance company, and AllClear Identity Repair is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur.
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud.
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of AllClear Identity Repair coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the eligibility database for AllClear Identity Repair, please contact AllClear ID:

E-mail	**Mail**	**Phone**
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077