



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

RECEIVED  
JUL 30 2018  
CONSUMER PROTECTION

Sian M. Schafle  
Office: 267-930-4799  
Fax: 267-930-4771  
Email: [sschafle@mullen.law](mailto:sschafle@mullen.law)

1275 Drummers Lane, Suite 302  
Wayne, PA 19087

July 20, 2018

**INTENDED FOR ADDRESSEE(S) ONLY**

**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 Event**

Dear Attorney General Gordon J. MacDonald:

We represent Boys Town National Research Hospital (“Boys Town”), 14100 Crawford Street, Boys Town, Nebraska, 68010, and are writing to notify you of a recent incident that may affect the security of the personally identifiable information (“PII”) of one (1) New Hampshire resident. Boys Town’s response to this incident is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Boys Town does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.

#### **Nature of the Data Event**

On May 23, 2018, Boys Town became aware of unusual activity relating to an employee email account. Boys Town immediately launched an investigation to determine what may have happened and what information may have been affected, working with computer forensics experts. The investigation determined that an unknown individual had access to the email account of a Boys Town employee on May 23, 2018. Boys Town reviewed the email account to identify what personal information was stored within the email account. Boys Town was unable to determine which emails the unauthorized individual may have opened or viewed.

Attorney General Gordon J. MacDonald

July 20, 2018

Page 2

An intensive forensic review of the contents of the impacted email account was performed to identify individuals for whom personally identifiable information (“PII”) and protected health information (“PHI”) was contained within the impacted email account at the time of potential unauthorized access. This effort required significant time and resources given the various document types and formatting of the items stored within the email account. On July 3, 2018, Boys Town confirmed the identities of individuals and entities whose PII and PHI were present in the email account. Boys Town then took steps to confirm the appropriate contact information for these individuals and entities for purposes of providing notification of the event.

The types of PII stored within the impacted email account were not identical for every potentially affected individual and/or entity. The PII for the impacted New Hampshire resident includes name and Social Security number.

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

On July 13, 2018, Boys Town began providing notice of this incident to individuals identified as having PII and PHI present in the email account at the time of the event. Required notifications continued through July 20, 2018, as Boys Town worked to confirm appropriate contact information for the notice recipients and establish resources to support these individuals and entities. Boys Town confirmed there was one (1) New Hampshire resident whose PII was present in the email account. The New Hampshire resident was provided notice of the event consistent with New Hampshire’s breach notification statute in substantially the same form as the letter attached hereto as *Exhibit A*. Boys Town also provided notice consistent with other applicable state and federal laws. Boys Town posted notice on its website and disseminated notice to media outlets on July 20, 2018, in substantially the same form as *Exhibits B & C*.

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

Boys Town is offering affected individuals complimentary access to 12 months of free credit monitoring and identity restoration services through AllClear ID. Additionally, Boys Town is providing potentially affected individuals with information on how to protect against identity theft and fraud, including information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, Boys Town will be providing notice to other state and federal regulators. Boys Town also reported this incident to law enforcement.

Boys Town has taken immediate steps to protect against similar incidents in the future. They reset passwords for Boys Town email accounts, implemented increased security measures for email account access, conducted additional employee training, and reviewed their company policies and procedures relating to data security.

Attorney General Gordon J. MacDonald

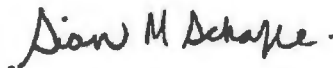
July 20, 2018

Page 3

**Contact Information**

Should you have any questions regarding this notification or other aspects of the data security incident, please contact me at (267) 930-4799.

Very truly yours,

A handwritten signature in black ink that reads "Sian M. Schafle." The signature is written in a cursive style.

Sian M. Schafle of  
MULLEN COUGHLIN LLC

SMS:af  
Enclosure

# EXHIBIT A



00001  
ACD1234

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

July 20, 2018

**Re: Notice of Data Breach**

Dear John Sample:

Boys Town National Research Hospital (“Boys Town”) is writing to notify you of an incident that may affect the security of some of your personal information. We take this incident very seriously. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so.

**What Happened?** On May 23, 2018, Boys Town became aware of unusual activity relating to an employee email account. We quickly launched an investigation to determine what may have happened and what information may have been affected, working together with computer forensics experts. Our investigation determined that an unknown individual had access to the email account on May 23, 2018. We reviewed the email account to identify what personal information was stored within the email account. Although we are unaware of any actual or attempted misuse of your personal information, we are providing you this notification out of an abundance of caution because your information was present in the account on May 23, 2018.

**What Information Was Involved?** Our investigation confirmed the information present in the impacted email account includes your name and ( ).

**What Are We Doing.** Information privacy and security are among our highest priorities. Boys Town has strict security measures in place to protect information in our care. Upon learning of this incident, we quickly took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for Boys Town email accounts, implemented increased security measures for email account access, conducted additional employee training, and reviewed our company policies and procedures relating to data security. We also notified necessary regulatory and law enforcement bodies. In an abundance of caution, we are also notifying potentially affected individuals, including you, so that you may take further steps to best protect your personal information, should you feel it is appropriate to do so. Although we are not aware of any actual or attempted misuse of information as a result of this event, we arranged to have AllClear ID protect your identity for 12 months at no cost to you as an added precaution.

**What Can You Do.** You may review the information contained in the attached “Steps You Can Take to Protect Your Information.” You may also enroll to receive the identity protection services we are making available to you. Boys Town will cover the cost of this service; however, you will need to enroll yourself in this service.



01-02-1-00

***For More Information.*** We recognize that you may have questions not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 1-855-686-9425 (toll free), Monday through Saturday, 8:00 a.m. to 8:00 p.m., CT.

We sincerely regret any inconvenience this incident may cause you. Boys Town remains committed to safeguarding information in our care and we will continue to take proactive steps to enhance the security of our systems.

Sincerely,

A handwritten signature in black ink that reads "Nisha Nair". The signature is written in a cursive, flowing style.

Nisha Nair, J.D.  
Boys Town National Research Hospital Privacy Officer

## Steps You Can Take to Protect Your Information

### **Enroll in Credit Monitoring**

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 1-855-686-9425 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](http://enroll.allclearid.com) or by phone by calling 1-855-686-9425 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.

**Monitor Your Accounts.** You may take action to protect against possible identity theft or financial loss, should you feel it is appropriate to do so. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your bank account statements, credit or debit card statements, and health insurance policy statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity.

**Credit Reports.** 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](http://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.

**Fraud Alerts.** At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax Consumer Fraud Division  
P.O. Box 740256  
Atlanta, GA 30374  
1-888-766-0008  
[www.alerts.equifax.com](http://www.alerts.equifax.com)

Experian  
P.O. Box 2002  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289  
[www.transunion.com](http://www.transunion.com)

**Security Freeze.** You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee (typically \$5 to \$15 each) to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files.

