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

February 14, 2020

INTENDED FOR ADDRESSEE(S) ONLY

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 NCH Healthcare System, Inc. ("NCH"), located at 350 7th Street North, Naples, FL 34102, and are writing to notify your office of an incident that may affect the security of some personal information relating to three (3) New Hampshire residents. By providing this notice, NCH 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 around June 14, 2019, NCH became aware of suspicious activity related to its human resources, timekeeping, and payroll system. NCH immediately launched an investigation into the activity and subsequently determined that certain employees fell victim to an email phishing scheme that allowed an unauthorized actor to gain access to the employee's payroll records as well as their email accounts. Third party specialists undertook a diligent and time-consuming manual and programmatic review of the entire contents of the relevant email accounts to determine what data was present as the investigation was not able to determine if any email was actually viewed. On December 19, 2019 the review provided confirmation of the identities of those individuals who may have had information present within the email accounts under review. NCH then began the laborious task of populating address information for the affected individuals from its internal records system.

The information that could have been accessible includes name and Social Security number.

Notice to New Hampshire Residents

On or about February 14, 2020, NCH provided written notice of this incident to affected individuals, including three (3) 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

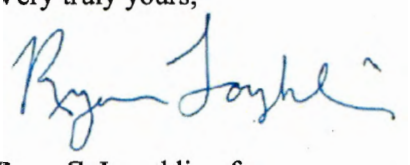
Upon discovering the event, NCH moved quickly to investigate and respond to the incident, assess the security of NCH systems, and notify potentially affected individuals. NCH is also working to implement additional safeguards and training to its employees. NCH is providing access to credit monitoring services for twenty-four (24) months through ID Experts, to individuals whose personal information was potentially accessible, at no cost to these individuals.

Additionally, NCH is providing 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. NCH 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. NCH is also notifying additional state regulators, as well as the U.S. Department of Health and Human Services about this event.

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:msf
Enclosure

EXHIBIT A

NCH Healthcare System

C/O ID Experts
PO Box 4219
Everett, WA 98204

To Enroll, Please Call:
1-833-554-0465
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

F3192-L02-0000002 P003 T00014 *********ALL FOR **** ###
<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

February 14, 2020

Dear <<First Name>> <<Last Name>>,

A cybersecurity forensic investigation firm hired by NCH Healthcare System recently wrapped up their investigation into an email phishing attack against our organization. You are receiving this letter to let you know that some personal information about you may have been accessible as a result of that attack.

What happened? On or around June 14, 2019, NCH became aware of suspicious activity related to our human resources, timekeeping, and payroll system. We immediately launched an investigation into this suspicious activity and determined that certain employees fell victim to an email phishing scheme that allowed an unauthorized actor (hacker) to gain access to the employee's payroll records as well as their email accounts. Importantly, NCH patient medical record systems were not affected by this incident, and the sole purpose of the attack appears to have been to reroute direct deposit payroll funds; however, the stolen credentials allowed access to employee email accounts. Third party specialists undertook a diligent and time-consuming manual and programmatic review of the entire contents of the relevant email accounts to determine what data was present as the investigation was not able to determine if any email was actually viewed. On December 19, 2019, the review provided confirmation of the identities of those individuals who may have had information present within the email accounts under review.

What information was involved? Our investigation determined the following information may have been accessible: <<data elements>>.

Who was affected? Certain NCH employee payroll and email accounts were subject to unauthorized access. However, to date, there has been no evidence of actual or attempted misuse of information present in the relevant email accounts. Nevertheless, out of an abundance of caution, we are providing you this notification because your information was present in one of the impacted email accounts.

What are we doing? The confidentiality, privacy, and security of personal information in our care is one of our highest priorities. Upon learning of the suspicious payroll activity, we immediately commenced an investigation and took steps to secure our systems. We worked with the third-party forensic investigators to confirm the full nature and scope of this event. We are notifying you of this event and providing you with information and resources to assist you in protecting your personal information. While we have measures in place to protect information in our systems, we are implementing additional safeguards to protect the security of information.

As an added precaution, we are offering you access to two years of credit monitoring and identity theft restoration services through ID Experts at no cost to you. Please review the attached "Steps You May Take to Protect Personal Information" for information on these services and instructions on how to enroll.

0000

What can you do? We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, monitoring your credit reports, and reviewing explanation of benefits forms for suspicious activity and errors. Please also review the enclosed "Steps You May Take to Protect Personal Information."

Again, while there has been no evidence to date of actual or attempted misuse of information present in the emails, we encourage you to register for the credit monitoring and identity theft restoration services offered by ID Experts at no cost to you for two years.

For more information. We understand you may have questions that are not answered in this letter. If so, please contact our dedicated assistance line at 1-833-554-0465, Monday through Friday, between 9 a.m. and 9 p.m. ET (excluding U.S. holidays).

We want to assure you that we take our responsibility to safeguard your personal information very seriously and apologize for any concern that this incident may have caused.

Sincerely,

Karen Sandrick

Karen Sandrick
Privacy Officer

STEPS YOU MAY TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Credit Monitoring

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-833-554-0465 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 9 a.m. - 9 p.m. ET. Please note the deadline to enroll is May 14, 2020.

Monitor Your Accounts

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 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
PO Box 105788
Atlanta, GA 30348-5788
1-800-349-9960
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 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-800-525-6285
www.equifax.com/personal/credit-report-services

0000

Additional Information

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 Maryland residents, the Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents, the Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Rhode Island Residents, the Rhode Island Attorney General may be contacted at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are two Rhode Island residents impacted by this incident.

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

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 violators. 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.