Pepper Hamilton LLP
Attorneys at Law

Suite 1200
4 Park Plaza
Irvine, CA 92614-2524
949.567.3500
Fax 949.863.0151

Sharon R. Klein
(949) 567-3506
kleins@pepperlaw.com

October 29, 2019

VIA OVERNIGHT MAIL
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: **Incident Notification**

Dear Attorney General MacDonald:

This firm represents Liberty Healthcare Corporation ("Liberty Healthcare"). Pursuant to New Hampshire Revised Statute §§ 359-C:20, we are writing to notify you of an incident involving unauthorized access to personal information involving one (1) New Hampshire resident.

Liberty Healthcare discovered that an external attacker gained access to a Liberty Healthcare employee's email account through the use of a phishing message on July 29, 2019. The phishing attack was successful at exposing only two email accounts, and the exposure was identified and the exposure eliminated within an hour of the initial incident. Liberty Healthcare undertook an investigation to identify the information that may have been accessed, and during the course of the ongoing investigation, recently discovered that the information of the New Hampshire resident could have been viewed. While Liberty Healthcare does not have any evidence that the attacker viewed any or all of the information in the emails contained in the employee's account, we are alerting you out of an abundance of caution because it is possible that the attacker could have viewed an email that contained the social security number, health insurance information or other personal information of the New Hampshire resident.

Following the incident, Liberty Healthcare immediately revoked the attacker's access by resetting the password and access token on each affected email account, and conducted a thorough investigation into the incident. Liberty Healthcare is continuing to proactively monitor its email accounts and at this time, is not aware of any other similar phishing emails or attacks. Liberty Healthcare intends to continue proactively educating and training its employees to prevent similar incidents from occurring in the future.

Liberty Healthcare anticipates notifying the New Hampshire resident affected no later than November 1, 2019. A copy of the notice being sent to the affected individual via U.S. first-class mail is attached as Exhibit A here. The letter advises the resident to monitor their credit reports and accounts; recommends that they place a fraud alert on their credit files and provides

instructions on how to do so; and provides contact information for Liberty Healthcare and encourages them to contact Liberty Healthcare with any additional questions.

Please rest assured that Liberty Healthcare takes its customers' privacy very seriously, and will continue to work diligently to protect their personal information. If you have any questions or require any additional information regarding this incident, please do not hesitate to contact me.

Sincerely,

Sharon R. Klein

Enclosure

Liberty Healthcare Corporation
THE FREEDOM TO SUCCEED™

800.331.7122
610.667.5559
liberty@libertyhealth.com
www.libertyhealthcare.com

EXHIBIT A

October [__], 2019

VIA MAIL

«SALUTATION» «FIRST» «LAST»
«ADDR1»
«ADDR2»
«CITY», «STATE» «ZIP»

Important Notice

Dear «SALUTATION» «LAST»,

What Happened:

We are writing to you because of a recent phishing incident at Liberty Healthcare Corporation. Late on July 29, 2019, we discovered that an external attacker gained access to an employee's email account through the use of a phishing message. As part of our ongoing investigation, we recently identified the possibility that your identifying information or health insurance policy information could have been exposed, as the account included emails containing your information.

What Information Was Involved:

While we do not have any direct evidence that any of your personal information was accessed, we are notifying you out of an abundance of caution because the attacker may have opened emails or attachments which could have contained your health insurance policy information.

What We Are Doing:

As soon as we became aware of the incident, we took corrective action to remediate any harm and to help prevent similar incidents from happening again, including changing the passwords for the affected email accounts and counselling our employees on how to identify and avoid phishing emails. Nonetheless, we felt it necessary to inform you since portions of your personal information may have been accessed.

As an extra precaution, to help protect your identity, we are offering a **complimentary** two-year membership of Experian's® IdentityWorks℠. Please see Exhibit A to this letter for instructions on how to enroll.

What You Can Do:

As a precautionary measure, we recommend that you remain vigilant by reviewing your financial account statements and credit reports closely. If you detect suspicious activity on any financial account, you should promptly notify the financial institution or the company with which the account is maintained.

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies is provided below:

Equifax
(800) 525-6285
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
(800) 680-7289
www.transunion.com
P.O. Box 2000
Chester, PA 19016

If you detect suspicious activity on any account, you should promptly notify the financial institution or company with which the account is maintained and report any suspected incidents of identity theft to local law enforcement authorities or your state attorney general. To report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft you can go to the FTC's Web site, at www.consumer.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338), or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

You also can contact the nationwide credit reporting agencies to place a security freeze to restrict access to your credit report altogether. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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, mortgages, employment, housing, or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800) 349-9960

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8872

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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit reporting agencies must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report or to remove the security freeze altogether, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

For More Information:

Should you need any further information about this incident, please contact Liberty's Privacy Office at 800.331.7122.

Sincerely,

Ms. Judith Shields
Privacy Officer

Exhibit A

Experian Enrollment Instructions

Activate Experian IdentityWorks in Three Easy Steps

1. Ensure that you **enroll by**: **«Experian_Exp_Date»** (Your code will not work after this date.)
2. **Visit** the Experian IdentityWorks website to enroll: **«Experian_URL»**
3. Provide your **activation code**: **«Experian_Personal_Code»**

If you have questions about the product, need assistance with identity restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **«Experian_Phone»** by **«Experian_Exp_Date»**. Be prepared to provide engagement number **«Experian_Engagement_»** as proof of eligibility for the identity restoration services by Experian.

Additional Details Regarding Your 24-Month Experian IdentityWorks Membership

A credit card is not required for enrollment.

You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.[1]
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: If selected, you receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance[2]:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Additionally, if you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this offer is available to you for two years from the date of this letter and does not require any action on your part at this time.

The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.