Dartmouth-Hitchcock

Dartmouth-Hitchcock
1 Medical Center Dr.
Lebanon, NH 03756-0001
Phone (603) 650-7676
Dartmouth-Hitchcock.org

January 20, 2014

Attorney General Michael A. Delaney
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Dartmouth-Hitchcock Medical Center – Incident Notification

Dear Attorney General Delaney:

I write to notify you of a data privacy incident at Dartmouth-Hitchcock ("D-H") that has affected the security of personal information of twelve (12) New Hampshire residents. D-H's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission.

On December 2, 2013, D-H discovered that, as a result of a phishing incident, certain D-H employee user accounts had unauthorized activity in the Employee Self Service Direct Deposit Payroll system. D-H immediately commenced an investigation of the incident and retained a third-party computer forensic company to investigate the extent of the unauthorized activity. Additional research indicates that the unauthorized access occurred from October 6, 2013 through December 2, 2013.

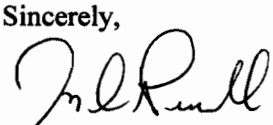
Since completing the forensic investigation, D-H has devoted considerable time and effort to determine what exact information may have been affected as a result of the phishing incident. D-H can confirm that full names and bank account information (routing and checking numbers) were compromised. In addition, as a result of the phishing incident, Social Security numbers were accessible through the Employee Self Service system. To date, however, D-H is not aware of any unauthorized acquisition of Social Security numbers. As a result, we wanted to make you (and the affected residents) aware of the incident and explain the steps we are taking to safeguard against identity fraud.

D-H provided the New Hampshire residents with written notice of this incident commencing on January 20, 2014, in substantially the same form as the letter attached hereto. D-H has advised the residents to monitor all credit reports and bank statements. D-H has offered a complimentary one-year membership in Experian's® ProtectMyID® to all affected residents. D-H is also providing a direct telephone number for additional support to those affected. D-H also advised the individuals affected to obtain a credit report and the process for placing a fraud alert on their credit files.

Maintaining the privacy of personal information is of the utmost importance to D-H. In light of this incident, D-H took steps with affected employees to secure against similar phishing occurrences by requiring that they change their passwords. In addition, D-H continues to monitor system activity and has implemented further security awareness for employees. D-H is also evaluating additional technical safeguards.

Should you have any questions regarding this notification or the incident, please contact at the address on the letter head above or via email at Martin.C.Purcell@Hitchcock.org.

Sincerely,



Martin Purcell
V.P. Information Services
Chief Security & Privacy Officer

Attachment

Dartmouth-Hitchcock

Dartmouth-Hitchcock
1 Medical Center Dr.
Lebanon, NH 03756-0001
Phone (603) 650-7676
Dartmouth-Hitchcock.org

January 20, 2014

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

XXXXXXXXXXX
YYYY
ZZZZ, YY 12345

Dear XXXXXX:

I am writing to you about a security incident involving your personal information that is maintained by Dartmouth-Hitchcock ("D-H").

As you may recall from conversations you had with D-H's Information Security team, on or around December 3, 2013, D-H discovered that, as a result of a phishing incident, certain D-H employee user accounts had unauthorized activity in the Employee Self Service Direct Deposit Payroll system. D-H immediately commenced an investigation of the incident and retained a third-party computer forensic company to investigate the extent of the unauthorized activity. Additional research indicates that the unauthorized access occurred from October 6, 2013 through December 2, 2013.

Since completing the forensic investigation, we have devoted considerable time and effort to determine what exact information may have been affected as a result of the phishing incident. We can confirm that your full name and bank account information (routing and checking numbers) were compromised. In addition, as a result of the phishing incident, your Social Security number may have been accessible through the Employee Self Service system, along with other information that you provided to D-H. To date, however, we are not aware of any unauthorized acquisition of your Social Security number. Nevertheless, we wanted to make you aware of the incident and explain the steps we are taking to safeguard you against identity fraud and suggest steps that you should take as well.

D-H takes this situation very seriously. We deeply regret that your personal information was involved in this incident. Maintaining the integrity of your confidential information is of the utmost importance to us. Enclosed you will find information on enrolling in a complimentary 12-month credit monitoring service along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and obtaining a free credit report. If you have not done so already, we advise you to please call your banking institution to determine if you should change your bank account number. In addition, we encourage you to carefully review your credit reports and financial statements.

In light of this incident, D-H took steps with you to secure against similar phishing occurrences by requiring that you change your password. In addition, D-H continues to monitor system activity and has implemented further security awareness for employees. D-H is also evaluating additional technical safeguards.

If you have any further questions regarding this incident, please call our IS Security Manager, Charles Goff, at 603-653-1380 or e-mail IS-Security@hitchcock.org.

Sincerely,

Martin Purcell
V.P. Information Services
Chief Security & Privacy Officer

Tina Naimie
V.P. Corporate Finance

1. **Enrolling in Complimentary 12 Month Credit Monitoring**

Protecting your personal information is important to D-H. In response to this security incident and as a precautionary measure, we have arranged for you to enroll in Experian's® ProtectMyID® Alert for a one year period at no cost to you. This protection is provided by Experian, one of the three major nationwide credit reporting companies.

Activate ProtectMyID Now in Three Easy Steps

1. ENROLL by **April 30, 2014**.
2. ENROLL at ProtectMyID Web Site, **www.protectmyid.com/redeem OR 877-371-7902**
3. PROVIDE your 9-character Activation Code: **XXXXXXXXX**

Once your ProtectMyID membership is activated, your credit report will be monitored daily for 50 leading indicators of identity theft. You'll receive timely Credit Alerts from ProtectMyID on any key changes in your credit report which could include new inquiries, new credit accounts, medical collections and changes to public records.

ProtectMyID provides you with powerful identity protection that will help detect, protect and resolve potential identity theft. In the case that identity theft is detected, ProtectMyID will assign a dedicated U.S.-based Identity Theft Resolution Agent who will walk you through the process of fraud resolution from start to finish for seamless service.

We realize that identity theft can happen months and even years after a data breach. To offer added protection, you will receive ExtendCARE™, which provides you with the same high-level of Fraud Resolution support even after your ProtectMyID membership has expired.

Your complimentary 12-month ProtectMyID membership includes:

- **Credit Report:** A free copy of your Experian credit report
- **Daily 3 Bureau Credit Monitoring:** Alerts you of suspicious activity including new inquiries, newly opened accounts, delinquencies, or medical collections found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution:** If you have been a victim of identity theft, you will be assigned a dedicated, U.S.-based Experian Identity Theft Resolution Agent who will walk you through the fraud resolution process, from start to finish.

- **ExtendCARE:** Full access to the same personalized assistance from a highly-trained Fraud Resolution Agent even after your initial ProtectMyID membership expires.
- **$1 Million Identity Theft Insurance:** As a ProtectMyID member, you are immediately covered by a $1 Million insurance policy that can help you cover certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of Chartis, Inc. 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.)

If you have any questions about ProtectMyID, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-371-7902.

2. Placing a Fraud Alert

Whether or not you choose to use the complimentary 12 month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

TransUnion
Consumer Fraud Division
PO Box 6790
Fullerton, CA 92834-6790
www.transunion.com/fraud
1-800-680-7289

Experian
Consumer Fraud Division
PO Box 9554
Allen, TX 75013
www.experian.com
1-888-397-3742

Equifax
Consumer Fraud Division
PO Box 740256
Atlanta, GA 30374-0256
www.equifax.com
1-800-525-6285

3. Obtaining a Free Credit Report

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit report online at **www.annualcreditreport.com**.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338) or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations.