BakerHostetler

STATE OF NH
DEPT OF JUSTICE
2015 FEB 13 AM 9:39

[redacted]

February 12, 2015

VIA OVERNIGHT DELIVERY

Office of the Attorney General
33 Capitol Street
Concord, NH 03301
Attn: Attorney General Joseph Foster

Re: Incident Notification

Dear Attorney General Foster:

On November 25, 2014, our client, Partners HealthCare System, Inc. and its affiliated institutions and hospitals ("Partners HealthCare"), learned that some Partners HealthCare workforce members may have provided their user credentials and answers to security challenge questions in response to phishing emails they received, thinking the emails were legitimate. When Partners HealthCare learned of this, it immediately began an investigation, contacted law enforcement and alerted the affected employees. Partners HealthCare also is working with an expert computer forensic firm to investigate the incident. Although the investigation is ongoing, Partners HealthCare believes that as a result of the phishing attack an unauthorized individual was potentially able to access information in its PeopleSoft system relating to some of its workforce members and their designated beneficiaries and dependents. The information potentially accessed with respect to workforce members included name, address, Social Security Number, date of birth, phone number, e-mail address, bank account number and bank routing number. With respect to beneficiaries and dependents, the information potentially accessed included name, address, date of birth, phone number, and Social Security number.

Partners HealthCare is notifying affected workforce members and their designated beneficiaries and dependents, and offering eligible individuals a complimentary one-year membership in credit monitoring and identity theft protection services from Experian. Partners HealthCare has also established a call center to assist individuals with any questions they may have.

Commencing on February 12, 2015, Partners HealthCare is notifying four New Hampshire residents pursuant to New Hampshire statute in substantially the same form as the letters attached hereto.[1]

To help prevent something like this from happening in the future, Partners HealthCare is continuing to re-enforce education with its workforce regarding phishing emails and is in the process of implementing enhancements for strengthening user login authentication to its systems.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

[redacted]

Enclosures

[1] This report is not, and does not constitute, a waiver of personal jurisdiction.

PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

{Insert Date}

{Insert Employee Name}
{Insert Employee Address}

Dear [First Name] [Last Name]:

Partners HealthCare System, Inc. and its affiliated institutions and hospitals ("Partners HealthCare") are committed to protecting the security and confidentiality of our workforce members' personal information. Regrettably, we are writing to inform you about an incident involving some of that information. We previously verbally informed you of this incident.

Partners HealthCare is comprised of various institutions and hospitals, including: Brigham and Women's Hospital, Brigham and Women's Faulkner Hospital, Massachusetts General Hospital, North Shore Medical Center, Partners Continuing Care, and Newton-Wellesley Hospital. On November 25, 2014, we learned that some Partners HealthCare workforce members may have provided their user credentials and answers to security challenge questions in response to phishing emails they received, thinking the emails were legitimate. When we learned of this, we immediately began an investigation and contacted law enforcement. We are also working with an expert computer forensic firm to investigate the incident. Although our investigation is ongoing, we believe that as a result of the phishing attack an unauthorized individual was potentially able to access information in our PeopleSoft system relating to some of our workforce members and their designated beneficiaries and dependents. The information potentially accessed included your name, address, Social Security Number, date of birth, phone number, e-mail address, bank account number and bank routing number.

We wanted to notify you regarding this incident and assure you that we take it very seriously. To help you detect possible misuse of your information, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We regret any inconvenience this may have caused you. To help prevent something like this from happening in the future, we are continuing to re-enforce education with our workforce regarding "phishing" emails and are in the process of implementing enhancements for strengthening user login authentication to our systems. If you have any questions, please call our Benefits Office at [redacted], Monday through Friday from 8:30 a.m. to 5:00 p.m. The toll-free number is [redacted]. Please dial our ten digit extension, when prompted, [redacted].

Sincerely,

Jigar Kadakia
Partners Chief Information Security and Privacy Officer

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: March 31, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **PC90693.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized 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.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. 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.

Information on Identity Theft Prevention

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

* 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.

Equifax	Experian	TransUnion
PO Box 740256	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

{Insert Date}

{Insert Name}
{Insert Address}

Dear [First Name] [Last Name]:

Partners HealthCare System, Inc. and its affiliated institutions and hospitals ("Partners HealthCare") are committed to protecting the security and confidentiality of the information we maintain on behalf of our workforce members and their beneficiaries and dependents. Regrettably, we are writing to inform you about an incident involving some of that information.

Partners HealthCare is comprised of various institutions and hospitals, including: Brigham and Women's Hospital, Brigham and Women's Faulkner Hospital, Massachusetts General Hospital, North Shore Medical Center, Partners Continuing Care, and Newton-Wellesley Hospital. On November 25, 2014, we learned that some Partners HealthCare workforce members may have provided their user credentials and answers to security challenge questions in response to phishing emails they received, thinking the emails were legitimate. When we learned of this, we immediately began an investigation and contacted law enforcement. We are also working with an expert computer forensic firm to investigate the incident. Although our investigation is ongoing, we believe that as a result of the phishing attack an unauthorized individual was potentially able to access information in our Human Resources system relating to some of our workforce members and also their designated beneficiaries and dependents. The information potentially accessed included your name, address, date of birth, phone number and Social Security number.

We wanted to notify you regarding this incident and assure you that we take it very seriously. To help you detect possible misuse of your information, we are offering a complimentary one-year membership of Experian's® ProtectMyID® Alert. This product helps detect possible misuse of your personal information and provides you with superior identity protection services focused on immediate identification and resolution of identity theft. ProtectMyID Alert is completely free to you and enrolling in this program will not hurt your credit score. Unfortunately, due to privacy laws, we are not able to enroll you directly. **For more information on identity theft prevention and ProtectMyID Alert, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.**

We regret any inconvenience this may have caused you. To help prevent something like this from happening in the future, we are continuing to re-enforce education with our workforce regarding "phishing" emails and are in the process of implementing enhancements for strengthening user login authentication to our systems. If you have any questions, please call our Benefits Office at [redacted], Monday through Friday from 8:30 a.m. to 5:00 p.m. The toll-free number is [redacted]. Please dial our ten digit extension, when prompted, [redacted].

Sincerely,

Jigar Kadakia
Partners Chief Information Security and Privacy Officer

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: April 30, 2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 877-371-7902 and provide engagement #: **PC91560.**

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH PROTECTMYID MEMBERSHIP:

A credit card is not required for enrollment.

Once your ProtectMyID membership is activated, you will receive the following features:

- **Free copy of your Experian credit report**
- **Surveillance Alerts for:**
  - **Daily Bureau Credit Monitoring:** Alerts of key changes & suspicious activity found on your Experian, Equifax® and TransUnion® credit reports.
- **Identity Theft Resolution & ProtectMyID ExtendCARE:** Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help with contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies.
  - It is recognized 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.
- **$1 Million Identity Theft Insurance*:** Immediately covers certain costs including, lost wages, private investigator fees, and unauthorized electronic fund transfers.

Once your enrollment in ProtectMyID is complete, you should carefully review your credit report for inaccurate or suspicious items. 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.

Information on Identity Theft Prevention

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

* 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.

Equifax	Experian	TransUnion
PO Box 740256	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

PARTNERS HEALTHCARE

FOUNDED BY BRIGHAM AND WOMEN'S HOSPITAL
AND MASSACHUSETTS GENERAL HOSPITAL

{Insert Date}

Parent or Guardian of [First Name] [Last Name]
{Insert Address}

Dear Parent or Guardian of [First Name] [Last Name]:

Partners HealthCare System, Inc. and its affiliated institutions and hospitals ("Partners HealthCare") are committed to protecting the security and confidentiality of the information we maintain on behalf of our workforce members and their beneficiaries and dependents. Regrettably, we are writing to inform you about an incident involving some of that information.

Partners HealthCare is comprised of various institutions and hospitals, including: Brigham and Women's Hospital, Brigham and Women's Faulkner Hospital, Massachusetts General Hospital, North Shore Medical Center, Partners Continuing Care, and Newton-Wellesley Hospital. On November 25, 2014, we learned that some Partners HealthCare workforce members may have provided their user credentials and answers to security challenge questions in response to phishing emails they received, thinking the emails were legitimate. When we learned of this, we immediately began an investigation and contacted law enforcement. We are also working with an expert computer forensic firm to investigate the incident. Although our investigation is ongoing, we believe that as a result of the phishing attack an unauthorized individual was potentially able to access information in our Human Resources system relating to some of our workforce members and their designated beneficiaries and dependents. Your child was designated as a beneficiary or dependent of one of our workforce members. The information potentially accessed included your child's name, address, date of birth, phone number and Social Security number.

We wanted to notify you regarding this incident and assure you that we take it very seriously. To help you detect the possible misuse of your child's information, we are providing you, the parent or guardian, with a complimentary one year membership in Family Secure® from Experian®. Family Secure monitors your Experian credit report to notify you of key changes. In addition, Family Secure will tell you if your child has a credit report, a potential sign that his or her identity has been stolen. To receive the complimentary Family Secure product, you as the parent or guardian must enroll at the web site with your activation code listed below. This activation code can only be used by the parent or guardian of the minor. Please keep in mind that once activated, the code cannot be re-used for another enrollment. **For more information on identity theft prevention and Experian's® Family Secure® Alert and instructions on how to activate your complimentary one-year membership, please see the included instructions in this letter.**

We regret any inconvenience this may have caused you. To help prevent something like this from happening in the future, we are continuing to re-enforce education with our workforce regarding "phishing" emails and are in the process of implementing enhancements for strengthening user login authentication to our systems. If you have any questions, please call our Benefits Office at [redacted], Monday through Friday from 8:30 a.m. to 5:00 p.m. The toll-free number is [redacted]. Please dial our ten digit extension, when prompted, [redacted].

Sincerely,

Jigar Kadakia
Partners Chief Information Security and Privacy Officer

Activate ProtectMyID Now in Three Easy Steps

1. ENSURE **That You Enroll By: 05/31/2015** (Your code will not work after this date.)
2. VISIT the **ProtectMyID Web Site: www.protectmyid.com/redeem**
3. PROVIDE **Your Activation Code: [code]**

If you have questions or need an alternative to enrolling online, please call 888-276-0529 and provide engagement #: PC91748.

What features does your 12-MONTH Family Secure membership include once activated?

Parent or Legal Guardian:

- Daily monitoring of your Experian credit report with email notification of key changes, as well as monthly "no-hit" reports
- 24/7 credit report access: Unlimited, on-demand Experian reports and scores
- Experian credit score illustrator to show monthly score trending and analysis.

Children:

- Monthly monitoring to determine whether enrolled minors in your household have an Experian credit report
- Alerts of key changes to your children's Experian credit report

All Members:

- Identity Theft Resolution assistance: Toll-free access to US-based customer care and a dedicated Identity Theft Resolution agent who will walk you through the process of fraud resolution from start to finish for seamless service. They will investigate each incident; help contacting credit grantors to dispute charges and close accounts including credit, debit and medical insurance cards; assist with freezing credit files; contact government agencies
- $2,000,000 Product Guarantee*

Once your enrollment in Family Secure is complete, you should carefully review your credit report for inaccurate or suspicious items. If you have any questions about Family Secure, 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 888-276-0529.

Information on Identity Theft Prevention

Even if you choose not to take advantage of this free credit monitoring service, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may also obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies. To order your credit report, free of charge once every 12 months, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	Experian	TransUnion
PO Box 740256	PO Box 9554	PO Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

* The Family Secure Product Guarantee is not available for Individuals who are residents of the state of New York.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov
1-877-438-4338

You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.