

# ALSTON & BIRD

The Atlantic Building  
950 F Street, NW  
Washington, DC 20004-1404  
202-239-3300 | Fax: 202-239-3333

RECEIVED

FEB 06 2018

CONSUMER PROTECTION

Kimberly K. Peretti

Direct Dial: 202-239-3720

Email: kimberly.peretti@alston.com

February 5, 2018

## **CONFIDENTIAL VIA OVERNIGHT DELIVERY**

Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: Notice of Security Incident

To the Office of the Attorney General:

We are writing on behalf of our client Partners HealthCare System, Inc. and its affiliated institutions and hospitals ("Partners"), to inform you of a potential security incident that may have involved unauthorized access to the personal information of 2 New Hampshire residents.

Partners' monitoring systems identified a sophisticated, malicious computer program on its computer network on May 8, 2017 and immediately blocked some of this malware. Working with internal and external forensics teams, Partners determined that the malware may have resulted in unauthorized access to certain data on affected computers between May 8, 2017 and May 17, 2017 and implemented aggressive containment measures to mitigate further impact.

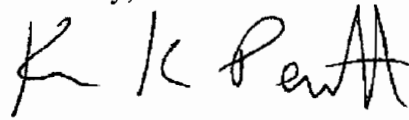
On July 11, 2017, we became aware of impacted data that appeared to be personal and health information. Because the impacted data was unstructured and consisted of a mix of computer code, dates, numbers, and other data, we undertook an extensive manual analysis. This review was completed in December of 2017. For some individuals, the affected personal information may have included first and last name, Social Security number and/or financial account information, in addition to protected health information. We are not aware of any misuse of personal or protected health information in connection with this incident.

In response to this incident, Partners has enhanced its security program, controls and procedures. Partners has also arranged for Experian to provide free credit monitoring services for one year to the individuals with Social Security numbers and/or financial account information affected.

A copy of the notification being sent to 2 New Hampshire residents on February 5, 2018 by first class mail is attached to this letter.

If you have any other questions regarding this incident or if you desire further information or assistance, please email me at [Kimberly.Peretti@alston.com](mailto:Kimberly.Peretti@alston.com) or call my direct line at (202) 239-3720.

Sincerely,

A handwritten signature in black ink, appearing to read "K Peretti". The signature is written in a cursive, somewhat stylized font.

Kimberly Peretti



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

Return Mail Processing  
PO Box 60  
Claysburg, PA 16625-0060



##D4801-L05-0123456  
SAMPLE A SAMPLE  
APT ABC  
123 ANY ST  
ANYTOWN, US 12345-6789

February 2, 2018

Dear Mr./Ms. Sample:

Partners HealthCare System, Inc. ("Partners") is deeply committed to protecting the security and confidentiality of personal and health information that we gather and maintain as part of our mission. Regrettably, we are writing to inform you of an incident involving some of that information.

On May 8, 2017, we became aware that our computer network had been affected by a sophisticated, malicious computer program introduced by an unauthorized third party. Our monitoring systems identified suspicious activity, and we immediately blocked some of this malware and began an investigation working with third party forensic consultants to identify the problem and mitigate its impact.

We were able to determine that the malware was not specifically targeted to impact the Partners environment, Partners operations or any information maintained by Partners. We also confirmed that there was no access to our electronic medical record system. As we continued the investigation, however, we became aware that the malware may have resulted in unauthorized access to certain data resulting from user activity on affected computers from May 8, 2017 to May 17, 2017. As impacted computers were identified, Partners implemented aggressive containment measures to mitigate further impact.

As part of our ongoing review, we became aware on July 11, 2017, of data that appeared to possibly involve personal and health information. The impacted data was not in any specific format, and it was mixed in together with computer code, dates, numbers and other data, making it very difficult to read or decipher. After an extensive manual data analysis that was completed in December 2017, we are reaching out to individuals whose personal and health information may have been involved out of an abundance of caution. Based on the review, this information may have included certain types of protected health information for some of our patients, including your first and last name, date(s) of service, and/or certain limited amounts of clinical information such as procedure type, diagnosis, and/or medication, as well as certain types of personal information for some of our patients, including your Social Security number and/or financial account information. *Importantly, we are not aware of any misuse of your personal or health information.*

0123456



We are enclosing with this letter a list of various steps that you can take to protect against potential misuse of your protected health information and to protect your identity. If you are a Massachusetts resident, you also have the following rights:

D4801-L05

- Right to obtain any police report filed in regard to this incident.
- Right to file a police report if you are the victim of identity theft and obtain a copy of it.
- Right to request that the credit bureaus place a security freeze on your file. Please refer to the enclosed information sheet for instructions on placing a security freeze on your credit report and additional steps you can take to further reduce any potential risk to you.

Additionally, we are offering you free credit monitoring and other services for a period of one year through Experian's IdentityWorks<sup>SM</sup>. More information on these Experian services, including instructions on how to activate the one-year of credit monitoring, is enclosed with this letter.

We deeply regret any inconvenience this may cause you, and Partners has enhanced its security program, controls and procedures as a result of this incident. If you have any questions, please call (877) 218-0056, Monday through Friday, between 9:00 a.m. and 7:00 p.m. Eastern Time (Closed on U.S. observed holidays). Please provide the following ten-digit reference number when calling: 2885020118.

Sincerely,



Jigar A. Kadakia  
Chief Information Security Officer  
Partners Healthcare System, Inc.

## **STEPS YOU CAN TAKE TO PROTECT YOUR PROTECTED HEALTH INFORMATION**

**Review Your Account Statements.** Carefully review statements sent to you from Partners as well as from your insurance company to ensure that all of your account activity is valid. Report any questionable charges promptly to the Partners Billing Office at the phone number listed on the statement, or for insurance statements, to your insurance company.

**Provide any updated personal information to your health care provider.** Your health care provider's office will ask to see a photo ID to verify your identity. Please bring a photo ID with you to every appointment if possible. Your provider's office will also ask you to confirm your date of birth, address, telephone, and other pertinent information so that we can make sure that all of your information is up-to-date. Please be sure and tell your provider's office when there are any changes to your information. Carefully reviewing this information with your provider's office at each visit helps us to avoid problems, and address them quickly should there be any discrepancies.

**Consult the Federal Trade Commission.** For more guidance on general steps you can take to protect your information, you also can contact the Federal Trade Commission:

Website: <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>  
Postal Address: Federal Trade Commission  
600 Pennsylvania Avenue, NW Washington, DC 20580  
Telephone: (202) 326-2222

0123456



## **STEPS YOU CAN TAKE TO PROTECT YOUR IDENTITY**

**Security Freeze.** A security freeze prohibits a credit bureau from releasing any information from your credit report without your written consent. Please be aware, however, that placing a security freeze on your credit report may delay or prevent the timely approval of any requests you make for new loans, credit, mortgages, or other services. To place a security freeze on your file, you must send a written request to each of the three credit bureaus by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze  
P.O. Box 105788  
Atlanta, GA 30348

Experian Security Freeze  
P.O. Box 9554  
Allen, TX 75013

TransUnion Security Freeze  
P. O. Box 2000  
Chester, PA 19016

When requesting a security freeze, you will need to provide the following information: (1) your full name; (2) your social security number; (3) your date of birth; (4) if you have moved in the past five years, the addresses where you have lived during that period; (5) proof of your current address, such as a current utility or telephone bill; and (6) a legible copy of your government-issued identification card, such as a state driver's license, state ID card, or military ID card. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, the credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. You will need to include payment by check, money order, or major credit card. Do not send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus also must send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both, that you can use 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, 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 to be available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those specific entities or individuals or for the specified period of time.

To remove the security freeze completely, you must send a written request to each of the three credit bureaus 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. The credit bureaus have three business days after receiving your request to remove the security freeze.

**Review Your Account Statements.** Carefully review your bank, credit card, and other account statements every month to ensure that all of your account activity is valid. Report any questionable charges promptly and in writing to the card or account issuer.

**Check Your Credit Report.** Check your credit report to ensure that all of your information is correct. You can obtain a free credit report once per year by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 877-322-8228. If you notice any inaccuracies, contact the relevant credit bureau promptly at the telephone number listed on the report. You can also report any suspicious activity to your local law enforcement, in which case you should request a copy of the police report and retain it for your records.

**Fraud Alert.** You have the right to request that the credit bureaus place a fraud alert on your file. A fraud alert tells creditors to contact you before opening any new accounts or increasing credit limits on your existing accounts. You need to contact only one of the three credit bureaus to place a fraud alert; the one you contact is required by law to contact the other two.

For Fraud Alerts, the credit bureaus can be reached at:

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

Experian  
P.O. Box 9532  
Allen, TX 75013  
888-397-3742  
www.experian.com

TransUnion  
P.O. Box 2000  
Chester, PA 19016  
888-909-8872  
www.transunion.com

**Consult the Federal Trade Commission.** For more guidance on steps you can take to protect your information, you also can contact the Federal Trade Commission at [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft), or at 877-ID-THEFT (877-438-4338), or at the Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, D.C. 20580.

0123456



## **Experian IdentityWorks<sup>SM</sup>**

To help you detect the possible misuse of your personal information, we are providing you with complimentary one year membership in Experian's IdentityWorks credit monitoring product at no cost to you.

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.

### **Activate EXPERIAN IDENTITYWORKS<sup>SM</sup> MEMBERSHIP Now in Three Easy Steps**

1. Ensure that you **enroll by: April 30, 2018** (After this date, your code will not work and you will not be able to enroll)
2. **Visit** the Experian IdentityWorks website to enroll: **<https://www.experianidworks.com/3bcredit>**
3. Provide your **activation code: ABCDEFGHI**

If you have questions or need an alternative to enrolling online, please contact Experian's customer care team at 877-890-9332 by April 30, 2018 and provide engagement #: **DB05151**

### **ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

The Experian IdentityWorks enrollment and services are provided at no cost to you.

A credit card is **not** required for enrollment in Experian IdentityWorks.

You have automatic and immediate access to fraud assistance through Experian. Contact Experian if you believe there was fraudulent use of your information. Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- ◆ **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- ◆ **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- ◆ **Experian IdentityWorks ExtendCARE<sup>TM</sup>:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- ◆ **\$1 Million Identity Theft Insurance<sup>\*\*</sup>:** Provides coverage for certain costs and unauthorized electronic fund transfers.

For additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s), refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration).