

RECEIVED
MAR 05 2018
CONSUMER PROTECTION

Mr. Joseph A. Foster
New Hampshire Department of Justice
Office Of The Attorney General
33 Capitol Street
Concord, NH 03301

March 1, 2018

Dear Attorney General Foster,

Please be advised that on January 26, 2018, an employee of ghg | GreyHealth Group sent certain employee records to an unauthorized email recipient. The documents contained certain personal information of individuals who were employed within ghg | GreyHealth Group in the United States in 2017, including names, home addresses, social security numbers and salary information.

It appears that 683 individuals could have been affected, including 1 individual who is a resident of your state. A draft copy of the notification to the affected individual is attached.

As set forth in the individual notification letter attached hereto, we are taking numerous steps to protect the security of the personal information of the affected individual, including implementing additional quality controls to avoid similar incidents in the future.

If you have any questions, please contact me at (917) 907-2406 or email erin.byrne@ghgroup.com.

Sincerely,



Erin Byrne
Chief Executive Officer



ghg | greyhealth group
200 Fifth Avenue
New York, NY 10010

February 15, 2018

##D5244-L01-0123456 0001 00000001 *****9-OELZZ 123

SAMPLE A SAMPLE - V1

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



NOTICE OF A DATA BREACH

WHAT HAPPENED?

We regret to inform you that ghg | GreyHealth Group was recently targeted in a phishing scam that resulted in an unauthorized party obtaining some of your personal information. First, I want to apologize that there has been an incident. Second, I want to ensure you that the company is taking this matter very seriously and has been, and will continue to, work tirelessly to investigate this incident and attempt to minimize the impact on you. My information was also disclosed, so I too am facing the same concerns and issues as you.

WHAT INFORMATION WAS INVOLVED?

Specifically, the security of the personal information of individuals who were employed within ghg | GreyHealth Group in the United States in 2017 has been compromised. Certain US employee records were sent to an unauthorized party on January 26, 2018, which the company discovered on February 6, 2018. The records were 2017 W2 tax forms which contained your name, home address, social security number and salary information.

WHAT WE ARE DOING.

Since discovering the unauthorized disclosure, we have been consulting with security experts, tax advisers, legal counsel and law enforcement, and will continue to consult with and evaluate their recommendations to best protect your personal information.

In an effort to minimize the effect that this incident may have on you, we have made arrangements to offer you identity theft and credit monitoring services for two years, at ghg | GreyHealth Group's expense. Specifically, we have procured Experian's Identity Restoration assistance and IdentityWorks services, which are now both available to you. Again, ghg | GreyHealth Group will cover the costs of these services, so we encourage you to take advantage of them. More information about how to access these services is immediately below:

• **Identity Restoration:**

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent right away at 877-890-9332. 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 (including, as appropriate, helping you with contacting credit grantors to dispute charges and close

0123456



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 on this site.

- **IdentityWorks:**

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM as a complimentary two year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information please follow the steps below:

- Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/3bplus
- Provide your activation code: ABCDEFGHI
- Ensure that you enroll by: May 31, 2018. Your code will not work after this date.

If you have questions about IdentityWorks, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by May 31, 2018. Be prepared to provide engagement number **DB05337** as proof of eligibility for the identity restoration services by Experian.

Please also note the following additional details regarding your 24-MONTH EXPERIAN IDENTITYWORKS Membership:

- A credit card is **not** required for enrollment in Experian IdentityWorks.
- 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.*
 - **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
 - **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
 - **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
 - **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
 - **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

WHAT ELSE YOU CAN DO.

- **Order Free Annual Credit Reports**

You have the right to obtain a copy of your credit report for free once a year from each credit reporting agency by contacting one of the agencies listed below or by visiting www.annualcreditreport.com or by calling toll free 877-322-8228. Hearing impaired consumers can access TTY service at 800-821-7232. You may order one, two, or three reports at the same time, or you may stagger your requests during a 12-month period to keep an eye on the information in your reports. The three credit bureaus are:

Equifax
877-478-7625
www.equifax.com

Experian
888-397-3742
www.experian.com

TransUnion
800-680-7289
www.transunion.com

- **Place A 90-Day Fraud Alert On Your Credit File**

You also have the right to place an initial “fraud alert” on your credit file. A “fraud alert” lets creditors know that they should contact you before they open a new account in your name. You can do this by calling any one of the three credit reporting agencies at the number above. This will let you automatically place fraud alerts with all three agencies listed above. The “fraud alert” will stay on your account for 90 days. After that, you can renew the alert for additional 90-day periods by calling any of the three agencies.

- **Place A Security Freeze On Your Credit File**

If you are very concerned about becoming a victim of fraud or identity theft, a security freeze might be right for you. Placing a freeze on your credit report will prevent lenders and others from accessing your credit report entirely, which will prevent them from extending credit. With a security freeze in place, you will be required to take special steps when you wish to apply for any type of credit. This process must be completed by contacting each of the credit reporting companies.

OTHER IMPORTANT INFORMATION.

When you receive your credit report, look it over carefully. In particular, review the report for accounts you did not open, inquiries from creditors that you did not initiate and personal information, such as home address, employment or social security numbers, which is inaccurate. If you see anything that you do not understand, call the credit agency at the telephone number listed on the report. If you do find suspicious activity on your credit report, call your local police department and the Federal Trade Commission and file a report of identity theft. We encourage you to be vigilant about protecting yourself from fraud and identity theft. Please review the enclosed *Information about Identity Theft Protection*. For more information, please see <https://www.identitytheft.gov>.

Social security numbers can be used to open lines of credit or file false tax returns. While taking the steps outlined above can be helpful, and the IRS is well aware of common identity theft scams, you should be vigilant in attending to your accounts and financial matters. The IRS has improved their procedures over the past few years to identify fraudulent activity. They have posted online information and procedures regarding how to deal with identity theft with respect to the filing of tax returns. Please see: <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft>, and carefully review all applicable IRS information before submitting any forms or taking any actions. Please check with your state tax authorities for comparable information. In the event a fraudulent Return has been filed, you may not be able to e-file your Tax Return and will need to file a paper Return instead.

FOR MORE INFORMATION.

If you have any questions, you can contact me directly (erin.byme@ghgroup.com or 917-907-2406). You can also contact the Experian call center at 877-890-9332, Monday through Friday between 6 a.m. – 6 p.m. PT, or Saturdays/Sundays between 8 a.m. – 5 p.m. PT for more information.

Please be assured that we take the protection of your information very seriously. Again, we apologize for any inconvenience this incident may cause you.

Sincerely,



Erin Byrne
Chief Executive Officer

0123456



Information about Identity Theft Protection

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax: P.O. Box 740241, Atlanta, Georgia 30374-0241, 1-800-685-1111, www.equifax.com
Experian: P.O. Box 9532, Allen, TX 75013, 1-888-397-3742, www.experian.com
TransUnion: P.O. Box 1000, Chester, PA 19022, 1-800-888-4213, www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding identity theft.

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For residents of Massachusetts: You also have the right to obtain a police report.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office, Consumer Protection Division
9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put your creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax: 1-888-766-0008, www.equifax.com
Experian: 1-888-397-3742, www.experian.com
TransUnion: 1-800-680-7289, fraud.transunion.com

Credit Freezes (for Non-Massachusetts Residents): You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. *Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company.* Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC : P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above.

Credit Freezes (for Massachusetts Residents): Massachusetts law gives you the right to place a security freeze on your consumer reports. A security freeze is designed to prevent credit, loans and services from being approved in your name without your consent. Using a security freeze, however, may delay your ability to obtain credit. You may request that a freeze be placed on your credit report by sending a request to a credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com
Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com
TransUnion LLC : P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. The following information should be included when requesting a security freeze (documentation for you and your spouse must be submitted when freezing a spouse's credit report): full name, with middle initial and any suffixes; Social Security number; date of birth (month, day and year); current address and previous addresses for the past five (5) years; and applicable fee (if any) or incident report or complaint with a law enforcement agency or the Department of Motor Vehicles. The request should also include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a utility bill, bank or insurance statement. Each copy should be legible, display your name and current mailing address, and the date of issue (statement dates must be recent). The credit reporting company may charge a reasonable fee of up to \$5 to place a freeze or lift or remove a freeze, unless you are a victim of identity theft or the spouse of a victim of identity theft, and have submitted a valid police report relating to the identity theft to the credit reporting company.

0123456

