GOLD KEY|PHR™

[redacted]

IMPORTANT INFORMATION
PLEASE READ CAREFULLY

[redacted]

Dear [redacted]

The privacy of your personal information is of utmost importance to GoldKey|PHR. I am writing with important information about a recent incident involving the security of our employees' personal information. We wanted to provide you with information regarding the incident and explain the services we are making available to help safeguard you against identity fraud.

What Happened?

On April 3, 2016 we discovered that on February 29, 2016, as a result of a criminal phishing email, an unauthorized third party may have obtained an electronic file containing Form W-2s for each associate. Form W-2s contain certain personal information on each associate employed in 2015.

What Information Was Involved?

We have confirmed that the information obtained by the unauthorized party included your 2015 Form W-2, which included your full name, Social Security number, home address, and wage and tax withholding information.

What We Are Doing.

Upon learning of the issue, our incident response team promptly began an investigation, engaged cybersecurity professionals to assist us, and took steps to prevent further unauthorized access to employee records. We are aware some employees have reported tax fraud issues - when they filed their tax return, the Internal Revenue Service rejected the filing, stating someone had already filed or attempted to file their tax return. At this time, we cannot be certain that these instances are directly related to this incident. We want to make you aware of the incident, explain the services we are making available to help safeguard you against identity fraud, and suggest steps you should take.

What You Can Do.

Enclosed in this letter you will find information on enrolling in a 12-month membership of Experian's ProtectMyID® Alert, that we are providing at no cost to you, along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

The information that is likely to be most at risk in this situation is the type of information that may be used to file fraudulent tax returns. As a result, you should contact your tax advisor, if you have one, and let them know that this information may be at risk. You should also file your tax return as quickly as possible, if you have not already done so.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax return was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you contact your tax advisor, if you have one; file an Identity Theft Affidavit (Form 14039) with the IRS (the form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf); call the IRS at (800) 908-4490, ext. 245 to report the situation (the unit office is open Monday through Friday from 7 am to 7 pm); and report the situation to your local police department. Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection

As a reminder, always verify the email address and sender of any email you receive requesting confidential or sensitive information. If you have any doubt about a request for confidential information, you should contact the apparent requestor via telephone or in person to confirm the request.

For More Information.

If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [redacted]
This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against misuse of your information. The response line is available Monday through Friday, 8:00 am to 5:00 p.m. Eastern Time.

GoldKey|PHR is committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information, and have taken steps to prevent further unauthorized access to employee records. Please know that we are devoting considerable resources to ensure our employees are fully informed and protected as a result of this unfortunate incident.

Sincerely,

[redacted]

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

Protecting your personal information is important to GoldKey|PHR. 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 Experian's® ProtectMyID Now in Three Easy Steps:

1. ENSURE that you enroll by [redacted]
2. VISIT the ProtectMyID Web Site to enroll: [redacted]
3. PROVIDE your 9-character Activation Code: [redacted]

If you have questions or need an alternative to enrolling online, please call [redacted] and provide Engagement [redacted]

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 Identify 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 an incident. 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. (Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of 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.)

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 [redacted]

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, at no charge. 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.

Equifax
P.O. Box 105069
Atlanta, GA 30348
www.equifax.com
1-800-525-6285

Experian
P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022
www.transunion.com
1-800-680-7289

3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
PO Box 9554
Allen, TX 75013
http://experian.com/freeze
1-888-397-3742

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19022
http://www.transunion.com/securityfreeze
1-800-680-7289

If you decide to place a Security Freeze on your credit file, in order to do so without paying a fee you will need to provide a police report. If your personal information has been used to file a false tax return or to open an account or to attempt to open an account, you may file a police report in the City in which you currently reside.

4. 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 reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

5. Additional Helpful Resources.

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 Federal Trade Commission, Consumer Response Center, 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. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If you live in ***Maryland***, in addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

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

If you live in ***North Carolina***, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice
Office of the Attorney General
9001 Mail Service Center
Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com

6. Reporting Identity Fraud to the IRS.

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: https://www.irs.gov/pub/irs-pdf/f14039.pdf
- Call the IRS at (800) 908-4490, ext. 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at http://www.irs.gov/uac/Identity-Protection

McDonald Hopkins

A business advisory and advocacy law firm®

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304

METROPLEX
MI 480
20 APR '16
PM 5 L

UNITED STATES POSTAGE
PITNEY BOWES
02 1P $ 000.705
0003184298
MAILED FROM ZIP CODE 48304

RECEIVED
APR 25 2016
OFFICE OF CONSUMER PROTECTION

Montana Attorney General
Office of Consumer Protection
P.O. Box 200151
Helena, Montana 59620

59620015151