McDonald Hopkins
A business advisory and advocacy law firm®

STATE OF NH
DEPT OF JUSTICE
2016 MAR 15 AM 11: 22

McDonald Hopkins PLC
39533 Woodward Avenue
Suite 318
Bloomfield Hills, MI 48304
P 1.248.646.5070
F 1.248.646.5075

Dominic A. Paluzzi
Direct Dial: 248.220.1356
dpaluzzi@mcdonaldhopkins.com

February 26, 2016

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

Re: WorkCare – Incident Notification

Dear Attorney General Delaney:

McDonald Hopkins PLC represents WorkCare, Inc. ("WorkCare") located in Anaheim, California. I write to provide notification concerning an incident that affects the security of personal information of three (3) New Hampshire residents. WorkCare's investigation is ongoing and this notification will be supplemented with any new significant facts or findings subsequent to this submission, if any. By providing this notice, WorkCare does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 18, 2016, as a result of a phishing incident, an unauthorized third party received an electronic file containing certain information on all current and former employees of WorkCare. Upon learning of the issue, WorkCare's incident response team promptly launched an investigation. As part of its investigation, WorkCare has been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents.

We have confirmed that the information that was received by the unauthorized party included employees' names, Social Security numbers, home addresses, salary, and tax withholding information.

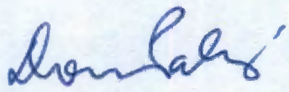
As a result, WorkCare wanted to notify you (and the affected residents) about this incident and explain the services they are making available to safeguard residents against identity fraud. WorkCare provided the New Hampshire residents with written notice of this incident commencing on February 26, 2016, in substantially the same form as the letter attached hereto. WorkCare has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. WorkCare is also offering the residents a complimentary two-year membership with a credit monitoring and identity theft protection service and is providing dedicated call center support to answer questions. WorkCare has advised the residents about the process for placing a fraud alert on their credit files, placing a security freeze, and

obtaining a free credit report. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

WorkCare takes its obligation to protect personal information very seriously. WorkCare is continually evaluating and modifying its practices to enhance the security and privacy of personal information, including training its workforce on security threats.

Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,



Dominic A. Paluzzi

DAP/kjb
Encl.

Human Resources Department
300 S. Harbor Blvd., Suite 600
Anaheim, CA 92805

NOTICE OF DATA BREACH

<<mail id>>
<<Name1>>
<<Name2>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Dear <<First Name>>,

The privacy of your personal information is of utmost importance to WorkCare, Inc. I am writing to you 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 let you know that we continue to take significant measures to protect your information.

What Happened?

On February 18, 2016, as a result of a phishing incident, an unauthorized third party received an electronic file containing certain information on all of our current and former employees, including myself.

What Information Was Involved?

We have confirmed that the information that was received by the unauthorized party included your full name, Social Security number, home address, salary, and tax withholding information. No other financial or medical information was acquired.

What We Are Doing.

Upon learning of the issue, our incident response team promptly launched an investigation. As part of our investigation, we have been working very closely with external cybersecurity professionals who regularly investigate and analyze these types of incidents. Out of an abundance of caution, we wanted to make you aware of the incident, explain the services we are making available to safeguard you against identity fraud, and suggest steps that you should take as well.

We want to assure you that WorkCare, Inc. is taking the steps necessary to ensure the security of our systems in response to this incident.

What You Can Do.

Enclosed you will find information on enrolling in a 24-month membership for Experian's ProtectMyID® Alert, which is a credit monitoring and identity theft resolution service 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/or 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.

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 (844) 746-4694. 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, 6:00 a.m. to 6:00 p.m. Pacific Time.

If you would like to speak to someone from WorkCare, Inc. regarding this incident, please contact me at 714-456-2108 or Allison Khosroshahin, Director HR, at 714-456-2121.

Please accept my sincere apologies that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information, including training our workforce on security threats.

Sincerely,

William E. Nixon
Chief Financial Officer
WorkCare, Inc.

–OTHER IMPORTANT INFORMATION–

1. **Enrolling in Complimentary 24-Month Credit Monitoring.**

Protecting your personal information is important to WorkCare, Inc. 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 two-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 **May 31, 2016.**
2. VISIT the ProtectMyID Website to enroll: **www.protectmyid.com/redeem**
3. PROVIDE your 9-character Activation Code: **<<Account Code>>**

If you have questions or need an alternative to enrolling online, please call 877-288-8057 and provide Engagement # **PC99496**.

Additional Details Regarding Your 24-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 and suspicious activity found on your Experian, Equifax®, and TransUnion® credit reports.
- **Identity Theft Resolution and ProtectMyID ExtendCARE:** Toll-free access to U.S.-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; and 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, 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 877-288-8057.

2. **Placing a Fraud Alert.**

Whether or not you choose to use the complimentary 24-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	**Experian**	**TransUnion**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	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

4. **Obtaining a Free Credit Report.**

Under federal law, you are entitled to one free credit report every twelve 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, D.C. 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 are a ***MARYLAND*** resident, please read the following:

In addition to the FTC, the Maryland Office of the Attorney General can 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 are a ***NORTH CAROLINA*** resident, please read the following:

In addition to the FTC, the North Carolina Office of the Attorney General can 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

Instances of known or suspected identity theft should also be reported to law enforcement.