McDonald Hopkins
A business advisory and advocacy law firm®

STATE OF NH
DEPT OF JUSTICE
2017 FEB 28 AM 11:09

**James J. Giszczak**
Direct Dial: 248.220.1354
jgiszczak@mcdonaldhopkins.com

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

February 24, 2017

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

**Re: Ashland University – Incident Notification**

Dear Attorney General Foster:

McDonald Hopkins PLC represents Ashland University. I write to provide notification concerning an incident that may affect the security of personal information of two (2) New Hampshire residents. Ashland University'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, Ashland University does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On February 8, 2017, Ashland University discovered that on February 3, 2017, as a result of a criminal phishing email, an unauthorized third party obtained an electronic file containing 2016 Form W-2s of current and some former employees of Ashland University. Upon learning of the issue, Ashland University's incident response team promptly began an investigation, notified law enforcement, engaged cybersecurity professionals to assist in the response, and took steps to prevent further unauthorized access to employee records.

Ashland University has confirmed that the information obtained by the unauthorized party included 2016 Form W-2s, which included residents' full names, Social Security numbers, home addresses, and wage and tax withholding information for 2016.

To date, Ashland University is not aware of any instances of identity fraud as a direct result of this incident. Nevertheless, we wanted to make you (and the affected residents) aware of the incident and explain the steps Ashland University is taking to safeguard the residents against identity fraud. Ashland University provided the New Hampshire residents with written notice of this incident commencing on February 24, 2017, in substantially the same form as the letter attached hereto. Ashland University is offering the residents a complimentary membership with a credit monitoring and identity theft restoration service and also is providing dedicated call center support to answer questions. Ashland University has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Additionally, Ashland University has advised the residents about the process for obtaining a free credit report, placing a fraud alert and/or security freeze on their credit files, and the process for

reporting identity theft to the IRS. The residents have also been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Ashland University is committed to maintaining the privacy of personal information and has taken many precautions to help safeguard it. Ashland University is continually evaluating and modifying its practices to enhance the security and privacy of personal information, and has taken steps to prevent further unauthorized access to employee records. In light of this incident, Ashland University will implement measures to prevent recurrence of this situation, including ongoing workforce training on privacy matters.

Should you have any questions regarding this notification, please contact me at (248) 220-1354 or jgiszczak@mcdonaldhopkins.com.

Sincerely,

James J. Giszczak

JJG/sdg
Encl.

[redacted]

February 24, 2017

***IMPORTANT INFORMATION***
***PLEASE READ CAREFULLY***

[redacted]

Dear [redacted],

The privacy of your personal information is of utmost importance to us. 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 February 8, 2017, we discovered that on February 3, 2017, as a result of a criminal phishing email, an unauthorized third party obtained an electronic file containing 2016 Form W-2s of current and some former employees of Ashland University. A Form W-2 is a wage and tax statement filed by your employer which contains your name and other personal information.

*What Information Was Involved?*

We have confirmed that the information obtained by the unauthorized party included your 2016 Form W-2, which included your full name, Social Security number, home address, and wage and tax withholding information for 2016.

*What We Are Doing.*

Upon learning of the issue, our incident response team promptly began an investigation, notified law enforcement, engaged cybersecurity professionals to assist us, and took steps to prevent further unauthorized access to employee records.

To date, we are not aware of any instances of identity fraud as a direct result of this incident. Nevertheless, we wanted to notify you about this incident, explain the services we are making available to safeguard you against identity fraud, and suggest steps that you should take as well.

*What You Can Do.*

Enclosed in this letter you will find information on enrolling in a 12-month membership of Equifax Credit Watch™ Gold, which we are providing at no cost to you, along with other precautionary measures we encourage you to take to help 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.

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 is 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 [redacted] 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. ***Additional instructions for filing the Affidavit (Form 14039) are included on the following pages.***

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 help protect against misuse of your information. The response line is available Monday through Friday, 9:00 a.m. to 9:00 p.m. Eastern Time.**

We are 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]

Stephen R. Storck
Vice President and Chief Financial Officer
Ashland University

## – ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

### 1. Enrolling in Complimentary 12-Month Credit Monitoring.

EQUIFAX®

**Activation Code:** [redacted]

| About the Equifax Credit Watch™ Gold identity theft protection product | Equifax Credit Watch provides you with the following key features and benefits: |
|---|---|
| Equifax Credit Watch will provide you with an "early warning system" to changes to your credit file. Note: You must be over age 18 with a credit file in order to take advantage of the product. | o Comprehensive credit file monitoring and automated alerts of key changes to your **Equifax** credit report<br>o Wireless alerts and customizable alerts available (available online only)<br>o Access to your Equifax Credit Report™<br>o Up to $25,000 in identity theft insurance with $0 deductible, at no additional cost to you †<br>o Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m.to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information.<br>o 90 day Fraud Alert placement with automatic renewal functionality* (available online only) |

**How to Enroll: You can sign up online or over the phone**

| To sign up online for **online delivery** go to [redacted] | To sign up for **US Mail delivery**, dial [redacted] for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only. |
|---|---|
| 1. Welcome Page: Enter the Activation Code provided at the top of this page in the "Activation Code" box and click the "Submit" button.<br>2. Register: Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the "Continue" button.<br>3. Create Account: Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the "Continue" button.<br>4. Verify ID: The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button.<br>5. Order Confirmation: This page shows you your completed enrollment. Please click the "View My Product" button to access the product features. | 1. Activation Code: You will be asked to enter your enrollment code as provided at the top of this letter.<br>2. Customer Information: You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.<br>3. Permissible Purpose: You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.<br>4. Order Confirmation: Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information. |

† Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. 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. This product is not intended for minors (under 18 years of age).

* The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

You must sign-up for this credit monitoring before [redacted]. You will not be able to enroll after this date.

## 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 LLC**
P.O. Box 2000
Chester, PA 19016
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
1-800-349-9960 (NY residents only)

**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 19016
http://www.transunion.com/securityfreeze
1-888-909-8872

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

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

**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:

- **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)**
    - *Instructions for Form 14039* – In Section A check box 1. / In Section B check box 2. / Insert this in the "Please provide an explanation" box: My company informed me that a third party unlawfully obtained an electronic file [W-2] containing certain employee personal information through a "phishing" scheme
- 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);
- Contact your tax preparer, if you have one; and/or
- You may call or visit your local law enforcement agency and file a police report. Please bring this notice with you.

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

**7. Reporting Identity Fraud to the Social Security Administration.**

If you believe that you are a victim of identity fraud AND it is affecting your Social Security account or records, you may contact the Social Security Administration at 1-800-772-1213 or visit https://secure.ssa.gov/acu/IPS_INTR/blockaccess. You also may review earnings posted to your record on your Social Security Statement on www.socialsecurity.gov/myaccount.

- The Social Security Administration has published Identity Theft and Your Social Security Number at: https://www.ssa.gov/pubs/EN-05-10064.pdf.