McDonald Hopkins

A business advisory and advocacy law firm®

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 23, 2018

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106

Re: Mize Houser & Company, P.A. – Incident Notification

Dear Sir or Madam:

McDonald Hopkins PLC represents Mize Houser & Company, P.A. ("Mize Houser"). I write to provide notification concerning an incident that may affect the security of personal information of one thousand five hundred sixty two (1,562) Iowa residents. Mize Houser'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, Mize Houser does not waive any rights or defenses regarding the applicability of Iowa law or personal jurisdiction.

On February 7, 2018, Mize Houser learned that W2s may have been damaged during the mailing process which may have allowed personal information to be viewable. Upon learning of the issue, Mize Houser commenced a prompt and thorough investigation. Mize Houser's third party printing and mailing vendor acknowledged an error with the paper they used and corrected W2s are in the process of being re-mailed to each individual.

Mize Houser confirmed that the information that was contained in the 2017 W2 that may have been damaged included name, address, tax and earnings information, and Social Security number.

To date, Mize Houser is not aware of any reports 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 Mize Houser is taking to help safeguard the residents against identity fraud. Mize Houser provided the Iowa residents with written notice of this incident commencing on February 23, 2018, in substantially the same form as the letter attached hereto. Mize Houser is offering the residents a complimentary membership with a credit monitoring and identity theft protection service. Mize Houser has advised the residents to remain vigilant in reviewing financial account statements for fraudulent or irregular activity. Mize Houser 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 also have been provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

Mize Houser is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Mize Houser continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

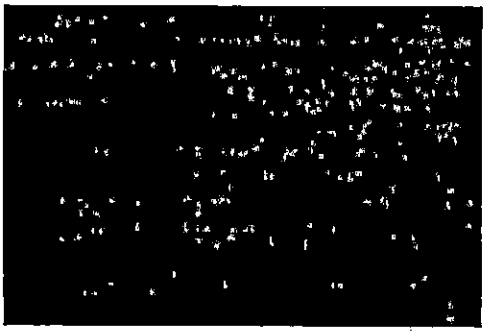
Should you have any questions regarding this notification, please contact me at (248) 220-1356 or dpaluzzi@mcdonaldhopkins.com.

Sincerely,

Dominic A. Paluzzi

Encl.

MIZE HOUSER & COMPANY, P.A.
534 S Kansas Ave.
Topeka, KS 66603



IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY

[redacted]

Dear [redacted]

I am writing with important information regarding a recent security incident. The privacy and security of the personal information belonging to our clients and their employees is of the utmost importance to Mize Houser & Company, P.A. ("Mize Houser"). Mize Houser maintains some of your personal information as it provides tax, payroll and accounting services to your employer. We wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened?

In early February, we learned that your W2 may have been damaged during the mailing process which may have allowed personal information to be viewable. Upon learning of the issue, we commenced a prompt and thorough investigation. Our third party printing and mailing vendor acknowledged an error with the paper they used and corrected W2s are in the process of being re-mailed to each individual.

What Information Was Involved?

The information that was contained in the 2017 W2 that may have been damaged included your name, address, tax and earnings information, and Social Security number.

What We Are Doing.

We have no reason to suspect that any of the information in the W2 has been or will be acquired or misused by any unauthorized individual. Nevertheless, out of an abundance of caution, we want to make you aware of the incident.

What You Can Do.

To protect you and your information, we are providing you with 12 months of free credit monitoring and identity theft protection services through TransUnion. This service helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. This service is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention, including instructions on how to activate your complimentary one-year membership, please see the additional information provided in this letter.

This letter also provides 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 and credit reports for fraudulent or irregular activity on a regular basis.

For More Information.

Please accept our apologies that this incident occurred. We are committed to maintaining the privacy of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal 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 potential misuse of your information. The response line is available Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time.

Sincerely,

Mize Houser & Company, P.A.

– OTHER IMPORTANT INFORMATION –

1. Enrolling in Complimentary 12-Month Credit Monitoring.

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for one year provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the *my*TrueIdentity website at [redacted] and in the space referenced as "Enter Activation Code", enter the following 12-letter Activation Code [redacted] and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at [redacted]. When prompted, enter the following 6-digit telephone pass code [redacted] and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and [redacted] Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain one year of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit files at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more.

The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion's secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child's Social Security Number. After TransUnion's search is complete, they will respond to you at the email address you provide. If they locate a file in your child's name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

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
Allen, TX 75013
https://www.freeze.equifax.com
1-800-685-1111

Experian Security Freeze
PO Box 9554
Atlanta, GA 30348
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

Please note that there may be a charge associated with placing, temporarily lifting, or removing a security freeze with each of the above credit reporting companies. These fees vary by state, so please call or visit the credit reporting agencies' websites to find out the specific costs applicable to the State in which you currently reside.

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 send a copy of a valid identity theft report or police report, by mail, to each credit reporting company to show that you are a victim of identity theft and are eligible for free security freeze services. If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the City in which you currently reside.

If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring. After you sign up for the credit monitoring service, you may refreeze your credit file. We encourage you to wait to place a security freeze on your credit file until you have enrolled in the credit monitoring service to avoid paying additional fees related to placing an initial security freeze on your credit file, temporarily lifting or removing the security freeze and subsequently refreezing your credit file.

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.

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

You may also report suspected incidents of identity theft to local law enforcement or the **Iowa Attorney General:**

Office of the Iowa Attorney General
Consumer Protection Division
1305 East Walnut Street
Des Moines, IA 50319
(515) 281-5164
1-888-777-4590
Fax: (515) 281-6771
www.iowaattorneygeneral.gov

6. Reporting Identity Fraud to the IRS.

If you believe 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 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.
- 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 or law enforcement department.

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