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

March 19, 2024

VIA U.S. MAIL

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Fiduciary Outsourcing, LLC – Incident Notification

To Whom it May Concern:

McDonald Hopkins PLC represents Fiduciary Outsourcing, LLC ("Fiduciary Outsourcing"), located at 2225 W. Whispering Wind Dr., Suite 200, Phoenix, AZ 85085. I am writing to provide notification of an incident at Fiduciary Outsourcing that may affect the security of personal information of approximately six (6) New Hampshire residents. Fiduciary Outsourcing is providing this notice and notice to individuals on behalf of certain business entity clients. Fiduciary Outsourcing will be supplement this notification with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, neither Fiduciary Outsourcing nor the clients on whose behalf this notice is made, waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Fiduciary Outsourcing received notice from a third-party vendor regarding a security vulnerability in the MOVEit Transfer solution which is utilized by Fiduciary Outsourcing. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer which has been actively exploited by unauthorized actors to gain access to access to data stored on MOVEit Transfer. There was no compromise of Fiduciary Outsourcing's broader network security.

Upon learning of this issue, Fiduciary Outsourcing immediately commenced an internal investigation and applied all to date security patches provided by Progress Software and revised the file retention configuration. Following the investigation, Fiduciary Outsourcing learned that certain data was obtained by an unauthorized actor and subsequently conducted a thorough review of the impacted data. This process was arduous as Fiduciary Outsourcing needed to identify all impacted data owners, individuals, data elements, and subsequently attribute the individual impacted to the appropriate entity. Fiduciary Outsourcing provided notice to the impacted entities and on or about March 1, 2024, received confirmation from certain entities to provide notice to individuals and regulators regarding the incident on the impacted entities' behalf. Information potentially impacted for New Hampshire residents included .

Fiduciary Outsourcing received updated mailing information for the impacted individuals on March 14, 2024, and effectuated notice as expeditiously as possible on or about March 19, 2024.

Fiduciary Outsourcing wanted to inform you (and the affected residents) of the incident on behalf of its clients and to explain the steps that it is taking to help safeguard the affected residents against identity fraud. Fiduciary Outsourcing is offering the residents whose Social Security number was impacted a complimentary membership with a credit monitoring service. Fiduciary Outsourcing will advise the affected residents to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Fiduciary Outsourcing will advise the affected residents about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected residents are also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission. Major credit reporting agencies have also been notified of the incident. A sample of the notification letter has been attached for reference.

At Fiduciary Outsourcing, protecting the privacy of personal information is a top priority. Fiduciary Outsourcing is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Fiduciary Outsourcing continually evaluates and modifies its practices to enhance the security and privacy of the personal information it maintains.

If you have any additional questions, please contact me at

Very truly yours,

Colin M. Battersby

Encl.

Fiduciary Outsourcing LLC
[redacted]

[redacted]

FIDUCIARY OUTSOURCING, LLC

March 19, 2024

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

Dear [redacted]

The privacy and security of the personal information entrusted to us is of the utmost importance to Fiduciary Outsourcing, LLC. We are writing to provide you with information regarding a recent incident that involves the security of some of your personal information that was supplied to us through the scope of our engagement with [redacted]. 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?
Fiduciary Outsourcing received notice from one of our third-party vendors regarding a security vulnerability in the MOVEit Transfer solution that is utilized by Fiduciary Outsourcing. Fiduciary Outsourcing is required to use secure transfer platforms to send and receive client data files to 401(k) record keepers and support payroll integration. On May 31, 2023, MOVEit reported a zero-day vulnerability in MOVEit Transfer that has been actively exploited by unauthorized actors to gain access to data stored on MOVEit Transfer. MOVEit has acknowledged the vulnerability and, as of June 2, 2023, provided patches to remediate the exploit. There was no compromise of Fiduciary Outsourcing's broader network security.

What We Are Doing.
Upon being informed of the vulnerability, Fiduciary Outsourcing immediately took actions to mitigate and assess the scope of information potentially compromised, including engaging third-party professionals to assist in the investigation and remediation of the vulnerability. Following our investigation, we discovered on March 1, 2024, that certain files that contain your personal information were potentially removed from our network by an unauthorized party.

What Information Was Involved?
The information that may have been accessed contained

What You Can Do.
We have no evidence that any of your information has been used to commit financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. In response to the incident, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for [redacted] months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to [redacted] and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted].

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

This letter also provides other precautionary measures you can take to protect your personal information, including placing a Fraud Alert and Security Freeze on your credit files, and 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 protect against misuse of your information. The response line is available for 90 days from the date of this letter, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays.

Sincerely,

Fiduciary Outsourcing LLC

- OTHER IMPORTANT INFORMATION -

1. Placing a Fraud Alert.

We recommend that you place a one-year "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 30348-5069
www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(888) 378-4329

Experian
P.O. Box 9554
Allen, TX 75013
www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
www.transunion.com/fraud-alerts
(800) 680-7289

2. 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 at no cost. 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
P.O. Box 105788
Atlanta, GA 30348-5788
www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze/center.html
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
www.transunion.com/credit-freeze
(888) 916-8800

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security number and other personal information such as copy of a government issued identification. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze. If you do place a security freeze prior to enrolling in a credit monitoring service, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

3. 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.

4. 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.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164. **Maryland Residents**: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.marylandattorneygeneral.gov, Telephone: 888-743-0023. **Massachusetts Residents**: Under Massachusetts law, you have the right to obtain a police report in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. **New Mexico residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov. **New York Residents:** You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755. **North Carolina Residents**: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000. **Oregon Residents**: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us, Telephone: 877-877-9392. **Rhode Island Residents**: You have the right to obtain a police report if one was filed, or alternatively, you can file a police report. Further, you can obtain information from the Rhode Island Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903, (401) 274-4400, www.riag.ri.gov. As noted above, you have the right to place a security freeze on your credit report at no charge, but note that consumer reporting agencies may charge fees for other services. To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above. In order to request a security freeze, you may need to provide the following information: your full name (including middle initial as well as Jr., Sr., II, III, etc.); Social Security number; date of birth; complete address; prior addresses; proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.); and if you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. When you place a security freeze on your credit report, within five (5) business days you will be provided with a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following: (1) the unique personal identification number or password provided by the consumer reporting agency; (2) proper identification to verify your identity; and (3) the proper information regarding the period of time for which the report shall be available to users of the credit report. There were 7 Rhode Island residents impacted. **Washington D.C. Residents**: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, oag.dc.gov/consumer-protection, Telephone: 202-442-9828.