McDonald Hopkins
A business advisory and advocacy law firm®

McDonald Hopkins LLC
300 N. LaSalle Street
Suite 1400
Chicago, IL 60654

P 1.312.280.0111
F 1.312.280.8232

April 2, 2024

VIA U.S. MAIL

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

Re: Haverford Township, PA – Incident Notification

To Whom it May Concern:

McDonald Hopkins PLC represents Haverford Township, PA ("Haverford") regarding a recent security incident. I am writing to provide notification of an incident at Haverford that may affect the security of personal information of approximately twelve (12) New Hampshire residents. Haverford's investigation is ongoing, and this notification will be supplemented with any new or significant facts or findings subsequent to this submission, if any. By providing this notice, Haverford does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

On or about April 17, 2023, Haverford became aware of potentially unauthorized access to their network due to a ransomware cybersecurity incident. Upon learning of the incident, Haverford Township immediately took steps to secure the network and mitigate against any additional harm. In addition, Haverford Township engaged external cybersecurity professionals experienced in handling these type of incidents to conduct an investigation. The forensic investigatory team learned that data potentially may have been removed by the unauthorized actor, however due to the limitations of available forensic evidence the forensic investigatory team could not determine the volume, if any, of data potentially acquired. Moreover, the forensic analysis did not indicate any evidence of data staging in the Haverford environment.

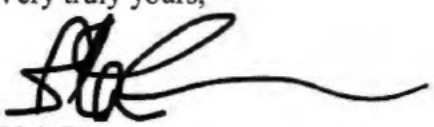
Nevertheless, out of an abundance of caution, Haverford Township engaged a vendor to conduct a thorough and extensive manual review of the potentially impacted data. Unfortunately, due to the unstructured nature of the potentially impacted data, this process has been arduous and time-consuming. Moreover, Haverford and the engaged data mining and manual review vendor encountered a number of issues loading and processing the potentially impacted data, which are required in order for review, resulting in continuous attempts to upload and process the potentially impacted data from August until approximately mid-November. The potentially impacted data was able to be successfully uploaded and processed by mid-November, at which time the data mining process commenced immediately thereafter, followed by a manual review of the potentially

impacted data. At the completion of the review, the vendor provided Haverford with a spreadsheet of potentially impacted individuals. Haverford determined on March 18, 2024, that the potentially impacted files may contain personal information of certain individuals including: . Not all information was affected for all individuals. On March 27, 2024, Haverford supplied notice to Pennsylvania media outlets and notice of the incident on its website. On March 28, 2024, Haverford located the most recent mailing addresses and on or about April 2, 2024, effectuated written notice via U.S. mail.

Haverford will be providing complimentary credit monitoring to those for whom their was potentially impacted. To date, Haverford Township has no evidence directly linking this incident to specific incidents of financial fraud or identity theft. Nevertheless, the potentially impacted individuals will also be advised regarding precautionary measures to best protect their identity and financial accounts including: remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis; the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports; and contact information for the consumer reporting agencies and the Federal Trade Commission. A sample of the notice letter is included herein for your reference.

At Haverford, protecting the privacy of personal information is a top priority. Haverford is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Further, Haverford continues to evaluate and improve, where appropriate, its administrative and technical safeguards including training its employees on best practices related to cybersecurity, policies, procedures, and protocols, and tools to protect its network environment. If you have any additional questions, please contact me at

Very truly yours,



Blair Dawson,
JD, MS CyS, FIP, CIPP/US, CIPP/E, CIPM

33404935.1

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

[redacted]

April 2, 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 Haverford Township, PA. We are writing to provide you with information regarding an incident which potentially involves the security of some of your personal information. As such, 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?
On or about April 17, 2023, Haverford Township detected unauthorized access to our network as a result of a cybersecurity incident that resulted in the potential exposure of the data we maintain.

What We Are Doing.
Upon learning of the incident, Haverford Township immediately took steps to secure the network and mitigate against any additional harm. In addition, we engaged external cybersecurity professionals experienced in handling these type of incidents to conduct an investigation. The forensic investigatory team learned that data potentially may have been accessed and/or removed by the unauthorized actor, however due to the limitations of available forensic evidence the forensic investigatory team could not determine the volume, if any, of data potentially accessed and/or acquired. Haverford Township has no evidence directly linking this incident to specific incidents of financial fraud or identity theft. Nevertheless, out of an abundance of caution, we conducted a thorough and extensive manual review of the potentially impacted data. After several months of extensive efforts to identify, review, and analyze the potentially impacted data, on March 18, 2024, Haverford Township determined that the potentially impacted files may contain personal information of certain individuals.

What Information Was Involved?
The information that may have been accessed contained some of your personal information, including your [redacted].

What You Can Do.
We have no evidence that any of your information has been used to commit identity theft or financial fraud. Nevertheless, out of an abundance of caution, we want to make you aware of the incident. We are providing you complimentary access to Identity Defense Complete for [redacted]* which includes the following key features: 1-Bureau Credit Monitoring, Monthly Credit Score and Tracker (VantageScore 3.0), Real-Time Authentication Alerts, High-Risk Transaction Monitoring, Address Change Monitoring, Dark Web Monitoring, Wallet Protection, Security Freeze Assist and $1 Million Identity Theft Insurance.**

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.
**Identity Theft Insurance is 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 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.

How to Enroll in Complimentary Credit Monitoring.
To enroll in Identity Defense, visit [redacted]

1. **Enter your unique Activation Code** [redacted]. Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account.** Enter your email address, create your password, and click 'Create Account'.
3. **Register.** Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation.** Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is [redacted]. After [redacted], the enrollment process will close, and your Identity Defense code will no longer be active. **If you do not enroll by** [redacted]**, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.** If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at [redacted].

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, 9am to 9pm ET.

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.

Sincerely,

Haverford Township, PA

– 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. Protecting Your Medical Information.

If this notice letter indicates that your medical information was impacted, we have no information to date indicating that your medical information involved in this incident was or will be used for any unintended purposes. As a general matter, however, the following practices can help to protect you from medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.
- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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.

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 seven 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.