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 14, 2023

VIA U.S. MAIL
John M. Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301

Re: Merritt Healthcare Advisors – Data Security Incident Notification

Dear Mr. Formella:

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

Merritt recently identified a data security incident involving unauthorized access to one Merritt employee's email account. Merritt is a healthcare advisory firm that provides services to healthcare organizations. Upon learning of the issue, Merritt secured the account and commenced a prompt and thorough investigation in consultation with external cybersecurity professionals who regularly investigate and analyze these types of incidents.

After an extensive forensic investigation and manual document review, Merritt discovered on November 30, 2022 that some personal information was contained in the account that was accessed between July 30, 2022 and August 25, 2022. Merritt advised its client covered entities of this incident on January 13, 2023. The accessed email account contained personal information of certain New Hampshire residents including their

Merritt has no evidence to suggest that any information has been acquired or misused as a direct result of this incident. Out of an abundance of caution, Merritt wanted to inform you (and the affected resident of the incident and to explain the steps that it is taking to help safeguard the affected resident against identity fraud. Merritt is providing the affected resident with written notification of this incident on March 14, 2023 in substantially the same form as the letter attached

hereto. Merritt will advise the affected resident to always remain vigilant in reviewing financial account statements for fraudulent or irregular activity on a regular basis. Merritt will advise the affected resident about the process for placing a fraud alert and/or security freeze on their credit files and obtaining free credit reports. The affected resident is also being provided with the contact information for the consumer reporting agencies and the Federal Trade Commission.

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

Notice is being provided pursuant to The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414.

If you have any additional questions, please contact me at

Sincerely,

Dominic A. Paluzzi

Encl.

Merritt Healthcare Advisors
INVESTMENT BANKING
P.O. Box 989728
West Sacramento, CA 95798-9728

[redacted]

[redacted]

March 14, 2023

Dear [redacted]

We are writing with important information regarding a recent data security incident that may have involved some of your personal information. Merritt Healthcare Advisors ("Merritt") is a healthcare advisory firm that provides services to healthcare organizations, including [redacted] The privacy and security of the information we maintain is of the utmost importance to Merritt. We wanted to provide you with information about the incident, the services we are making available to you, and to let you know that we continue to take significant measures to protect your information.

What Happened?

We recently learned that an unauthorized actor obtained access to a Merritt employee's email account.

What We Are Doing.

Upon learning of this issue, we secured the account and commenced a prompt and thorough investigation in consultation with external cybersecurity professionals who regularly investigate and analyze these types of incidents. After an extensive investigation and manual document review, we discovered on November 30, 2022 that some of your personal information was contained in the account that was accessed between July 30, 2022 and August 25, 2022. Merritt advised [redacted] of this incident on January 13, 2023.

What Information Was Involved?

The accessed email account contained some of your personal information, including your name and [redacted] Your Social Security number was not contained within the accessed account.

What You Can Do.

We have no evidence that any of your information has been acquired or misused as a direct result of this incident. Provided in the "Other Important Information"-portion of this letter are precautionary measures you can take to protect your personal information, including placing a fraud alert and/or security freeze on your credit files, 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. In addition, if this letter indicates that your medical information was involved, we have included steps you can take to protect such information.

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 additional 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 contact our toll-free incident response line at [redacted], Monday through Friday from 9 am to 9 pm Eastern Time.

Sincerely,

Merritt Healthcare Advisors

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

You may place an initial 1-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 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

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

TransUnion LLC
P.O. Box 6790
Fullerton,PA 92834-6790
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. 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 charge. 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 contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit- report-services/credit-freeze/
(800) 349-9960

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

TransUnion Security Freeze
P.O. Box 2000
Chester, PA 19016
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. 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.

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.

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 this letter indicates that your financial account number was impacted, we recommend that you contact your financial institution to inquire about ways in which you can protect your account, including obtaining a new account number.

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.

5. Protecting Your Medical Information.

In the event that your medical information was included in the accessed account, we have no information to date indicating that it 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.