

Heather Shumaker
Direct Dial: 248-402-4066
E-mail: hshumaker@mcdonalddhopkins.com

April 24, 2024

VIA ONLINE PORTAL

Aaron M. Frey
Office of the Maine Attorney General
Attn: Security Breach Notification
111 Sewall St
Augusta, ME 04330

Re: Moffitt Cancer Center and Research Institute – Advarra, Inc. Incident Notification

Dear Mr. Frey:

McDonald Hopkins PLC represents Moffitt Cancer Center and Research Institute (“Moffitt”). Advarra, Inc (“Advarra”) is a company that obtained patient information in connection with services provided to Moffitt related to the care and treatment of patients and research study. I am writing to notify you of a data security incident that occurred at Advarra that may affect the security of personal information of approximately twenty-four (24) Maine residents for whom it had a last known home address. By providing this notice, Moffitt does not waive any rights or defenses regarding the applicability of Maine law or personal jurisdiction.

On October 26, 2023, Advarra was made aware that an unauthorized third-party accessed a single Advarra employee’s user account, and acquired a limited amount of company data. Advarra promptly contained the incident by disabling the employee’s account and immediately launched an investigation into the nature and scope of the unauthorized access into its system. Through the investigation, Advarra learned that the unauthorized activity began on October 25, 2023. Advarra then conducted a review of the records to confirm the identities of individuals potentially affected by this event. With the assistance of external cybersecurity experts, Advarra has since taken a number of steps to enhance its information security.

After a thorough investigation, on February 21, 2024, Advarra notified Moffitt that the files downloaded by the third-party contained some information from Moffitt patients and study participants and on March 13, 2024, Moffitt completed its review of that information. The downloaded files contained individuals’ name, date of birth, and social security number. We want to assure you that this data security incident did not involve any access to Moffitt’s systems, networks or electronic health records.

Advarra informed Moffitt that it has implemented additional measures to further strengthen their internal files system. Additionally, Moffitt requested Advarra offer complimentary credit monitoring service at no cost to individuals. Advarra is providing the affected residents with written notification of this incident commencing on or about April 23, 2024 in substantially the same form as the letter attached hereto. Advarra is advising the affected residents about the process for placing fraud alerts and/or security freezes 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.

At Moffitt, protecting the privacy of personal information is a top priority. Moffitt is committed to maintaining the privacy of personal information in its possession and in the care of its business associates, requiring that they take precautions to safeguard it. Moffitt continually evaluates and modifies their practices to enhance the security and privacy of any personal information in its possession and in the care of its third party business associates.

Should you have any questions concerning this notification, please contact me at (248) 402-4066- or hshumaker@mcdonaldhopkins.com. Thank you for your cooperation.

Very truly yours,

A handwritten signature in black ink, appearing to read 'H. Shumaker', with a long, sweeping horizontal line extending to the right.

Heather Shumaker

Encl.



6100 Merriweather Dr., Suite 600
Columbia, MD 21044
410-884-2900

[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]

[REDACTED]

Dear [REDACTED]

Advarra, Inc (“Advarra”) is a company that obtained your information in connection with services provided to Moffitt Cancer Center related to the care and treatment of patients and research study participants. On behalf of Moffitt Cancer Center, we are writing to notify you of a data security incident that occurred at Advarra and involved some of your information. This notice explains the incident, measures taken to protect your information, and some steps you may consider taking in response. We regret that this incident occurred and apologize for any inconvenience.

What Happened?

On October 26, 2023, Advarra was made aware of a data security incident and immediately took measures to contain the incident. Following the incident, a thorough investigation was conducted, which revealed that on October 25, 2023, an unauthorized third-party accessed a single Advarra employee user account and acquired a limited amount of data. After we identified the files that were involved, we began a process to review those files to identify their content. This review process took several months to complete. Advarra notified federal law enforcement officials about the incident and has continued cooperating with them since the incident.

What Information Was Involved?

Advarra’s review of the files generated a preliminary list of individuals whose information was contained in the files. We then worked to review the list of individuals in order to identify them and the entities that originally supplied their information to Advarra. On or about February 8, 2024, Advarra completed its review of the list of individuals and confirmed that the downloaded files contained your: name, [REDACTED]. At the same time, Advarra confirmed that it originally obtained your information from Moffitt Cancer Center in connection with services Advarra was providing to Moffitt Cancer Center at the time.

On February 21, 2024, Advarra notified Moffitt Cancer Center that your personal information was involved during the data security incident and on March 13, 2024, Moffitt Cancer Center completed its review of that information. We want to assure you that this data security incident did not involve any access to Moffitt Cancer Center’s systems, networks or electronic health records.

What We Are Doing.

Upon learning of this incident, we took immediate steps to disable the affected account, launch a comprehensive investigation, and assess the security of our systems. We also engaged cybersecurity experts. We confirmed containment of the incident on October 26, 2023, and since then have seen no further unauthorized access to any portion of our network.

Advarra has implemented additional measures to further strengthen our internal files system. We have secured the services of Kroll to provide identity monitoring at no cost to you for 24 months. For more information on how to help safeguard your identity, including instructions on how to activate your complimentary membership, please visit the below website and see the additional information provided with this letter.

What You Can Do.

For more information on your complimentary membership to Kroll identity monitoring services, as well as additional steps you can take in response to this incident, please see the pages that follow this letter.

For More Information.

If you have any questions, please call [REDACTED] Monday through Friday, between 9:00 am and 6:30 pm, Eastern Time, excluding some U.S. holidays.

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report

may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state attorney general. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state attorney general. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. Fees may be required to be paid to the consumer reporting agencies. There are approximately [X] Rhode Island residents impacted by this event.

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.

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.

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.

Sincerely,

Advarra