



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

Sian M. Schafle
Office: (267) 930-4799
Fax: (267) 930-4771
Email: sschafle@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 26, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent Mount Carmel Care Center (“Mt. Carmel”) located at 320 Pittsfield Rd, Lenox, MA 01240, and are writing to notify your office of an incident that may affect the security of certain personal information relating to five (5) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Mt. Carmel does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

Mt. Carmel became aware of suspicious activity involving their computer network and promptly began an investigation. The investigation determined the network had been accessed by an unknown actor between August 17, 2023, and October 15, 2023, and during this time files were copied. Mt. Carmel conducted an extensive and detailed review of the files to determine the content and to whom it relates. While the review was taking place, Mt. Carmel began providing notice of this incident consistent with the Health Insurance Portability and Accountability Act (HIPAA) out of an abundance of caution. On June 6, 2024, Mt. Carmel completed the review and validation of the data and confirmed the impacted files contained information including name and financial account information.

Notice to Maryland Residents

On December 14, 2023, Mt. Carmel posted notice of this incident on its website. On August 26, 2024, Mt. Carmel continued with its notice efforts by mailing notice letters to individuals for whom

it had sufficient address information. Notice of this incident has been provided to five (5) Maryland residents in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, Mt. Carmel moved quickly to investigate and respond to the suspicious activity, assess the security of Mt. Carmel systems, and notifying potentially impacted individuals. Further, Mt. Carmel notified federal law enforcement regarding the event. As part of its ongoing commitment to information security, Mt. Carmel is reviewing its policies and procedures, as well as assessing new cybersecurity tools, to reduce the risk of a similar incident from occurring in the future.

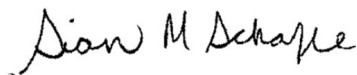
Mt. Carmel is providing these individuals with guidance on how to better protect against identity theft and fraud. Mt. Carmel is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Mt. Carmel is providing written notice of this incident to relevant state and federal regulators, as necessary. Mt. Carmel also provided media notice consistent with HIPAA in relevant jurisdictions.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4799.

Very truly yours,



Sian M. Schafle of
MULLEN COUGHLIN LLC

SMS/lcf
Enclosure

EXHIBIT A



9555 Avenue Christophe-Colomb
Montréal QC H2M 2E3

August 15, 2024

00695-ADFFIN G0326 L001 AUTO *000001



Dear

Mount Carmel Care Center ("Mt. Carmel") writes to inform you of an event that may involve some of your information.

This letter provides an overview of what happened, our response, and the resources available to you, should you feel it is necessary and appropriate to take additional action.

What Happened?

We became aware of suspicious activity involving our computer network and promptly began an investigation. The investigation determined that the network had been accessed by an unknown actor between August 17, 2023 and October 15, 2023, and during this time files were copied. As a result, we conducted a detailed review of the files to determine the type of information present and to whom it related, and on June 6, 2024 we completed the review. We are notifying you because the review identified some of your information.

What Information Was Involved?

The information identified in the involved files includes your name, account number with routing number, account number, and account number with bank name.

What We Are Doing.

We take this incident and the security of information in our care very seriously. We moved quickly to respond and investigate the suspicious activity, assess and secure our network, and notify potentially impacted individuals. As part of our ongoing commitment to information security, we are currently reviewing our policies and procedures, as well as assessing new cybersecurity tools, to reduce the risk of a similar incident from occurring in the future. We also notified federal law enforcement and will be notifying relevant regulators, as required.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits statements, and monitoring free credit reports for suspicious activity and to detect errors. Suspicious activity should be promptly reported to relevant parties including an insurance company, healthcare provider, and/or financial institution. Additional information and resources may be found below in the *Steps You Can Take to Protect Personal Information* section of this notice.

For More Information.

If you have any questions, please contact us at 1-888-244-3092 between 9am and 9pm Monday through Friday. You may also write to Mt. Carmel at 320 Pittsfield Rd, Lenox, MA 01240 or MCCdata@mcccl.org.

Sincerely,

Jodi Ouimette

Jodi Ouimette, Administrator
Mount Carmel Care Center



STEPS YOU CAN TAKE TO 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 1-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; 1-410-576-6300 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. There are approximately 3 Rhode Island residents that may be impacted by this event.



Test