David McMillan, Partner
Cybersecurity & Data Privacy Team
175 Pearl Street, Suite C-402
Brooklyn, New York 11201
dmcmillan@constangy.com
Direct: 718.614.8371

July 25, 2023

VIA ONLINE SUBMISSION
Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Life Management Center of Northwest Florida Inc. ("LMC") in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

On March 30, 2023, LMC became aware of unusual activity on its network. In response, LMC took immediate steps to secure its digital environment and engaged a leading cybersecurity firm to conduct an investigation to determine whether any sensitive information may have been accessed or acquired during the incident. Through the investigation, LMC learned that certain systems may have been accessed without authorization. Following this confirmation, LMC engaged a vendor to conduct a comprehensive review of the potentially affected data and on May 26, 2023, LMC determined that personal information belonging to certain individuals may have been impacted in connection with this incident. LMC then worked diligently to obtain contact information to effectuate notification to potentially affected individuals. This process was completed on June 15, 2023.

LMC is notifying all potentially impacted individuals of this incident, providing them with steps they can take to protect their personal information, and offering them free credit and identity monitoring services.

Please note that we have no current evidence to suggest misuse or attempted misuse of any personal information in conjunction with this incident.

2. **Number of Maine residents affected.**

LMC notified sixteen (16) Maine residents of this incident via first class U.S. mail on July 25, 2023. The information potentially impacted in connection with this incident includes name, and Social Security number.

A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as LMC discovered this incident, LMC took steps to secure its network environment and launched an investigation to determine what happened and the scope of personal information potentially impacted. LMC implemented measures to enhance the security of its environment in an effort to minimize the risk of a similar incident occurring in the future. In addition, LMC also notified the Federal Bureau of Investigation of the incident and will provide any cooperation necessary to help hold the perpetrator(s) accountable

Further, LMC has established a toll-free call center through Epiq, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-833-627-2717 from 6:00 A.M. to 6:00 P.M. PST on Monday through Friday (excluding holidays). In addition, while LMC is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, LMC is also providing complimentary credit and identity protection services to notified individuals.

4. Contact information.

LMC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact Constangy.

Best regards,

/s/ David McMillan

David McMillan
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Enclosure: Sample Notification Letter

Life Management Center
Of Northwest Florida Inc.

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

<<Mail ID>>
<<Name 1>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>

July 25, 2023

Subject: Notice of Data <<Variable Data 1>>

Dear <<Name 1>>:

We are writing to inform you about a recent data security incident experienced by Life Management Center of Northwest Florida Inc. ("LMC") that may have involved your personal and / or protected health information. LMC takes the privacy and security of all information within its possession very seriously. That is why we are writing to notify you of the incident, offer you complimentary credit monitoring and identity protection services, and provide you with information about steps you can take to help protect your information.

What Happened? On March 30, 2023, LMC detected unusual activity within our computer network. Upon discovery, LMC immediately took steps to secure its network and engaged a leading, independent digital forensics and incident response firm to investigate what happened and whether any sensitive data may have been impacted. Based on that investigation, LMC learned that an unknown actor gained unauthorized access to our network and may have acquired certain files, some of which may have contained individuals' personal and / or protected health information. LMC undertook a comprehensive review of the potentially impacted data to identify the individuals and information involved, which concluded on May 26, 2023. LMC then worked diligently to gather contact information for potentially impacted individuals and to provide notification as soon as possible.

What Information Was Involved? The information that was potentially impacted during this incident may have included your name, as well as your <<Breached Elements>>. Please note that LMC is not aware of any attempted or actual misuse of this information.

What Are We Doing? As soon as LMC discovered the incident, we took the steps described above and implemented measures to enhance the security of our network and reduce the risk of a similar incident occurring in the future. LMC also reported the incident to the Federal Bureau of Investigation and is cooperating any resulting investigation to hold the perpetrator(s) accountable.

While we have no evidence that any of your information was misused, out of an abundance of caution we are offering you complimentary credit monitoring and identity protection services through Equifax. These services include <<CM Duration>> months of credit[1] and dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. Additional details are included at the end of this letter.

[1] To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<Enrollment Deadline>> (Your code will not work after this date.)
- **Visit** the Equifax website to enroll: www.equifax.com/activate
- Provide your **activation code**: <<Enrollment Deadline>>

What Can You Do? We recommend that you review the guidance included in this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you through Equifax by using the activation code provided above.

For More Information: Further information about how to help protect your information appears on the following page. In addition, LMC has established a dedicated call center through Epiq to answer any questions about this matter and to provide assistance with enrolling in the complimentary services being offered to you. The call center can be reached at 833-627-2717 Monday through Friday from 6 am – 6 pm, Pacific Time (excluding major U.S. holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Retha M Threatt

Retha M. Threatt
Chief Human Resources Officer
Life Management Center of
Northwest Florida Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

California Attorney General
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550
https://oag.ca.gov/contact
1-916-210-6276

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

<<Name 1>>

Enter your Activation Code: <<*ACTIVATION CODE*>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of <<*ACTIVATION CODE*>> then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.