WHITEFORD, TAYLOR & PRESTON L.L.P.

SPENCER S. POLLOCK, CIPP/US, CIPM
CELL (410) 917-5189
Direct (410) 832-2002
spollock@wtplaw.com

SEVEN SAINT PAUL STREET
BALTIMORE, MARYLAND 21202-1636
MAIN TELEPHONE (410) 347-8700
FACSIMILE (410) 752-7092

DELAWARE*
DISTRICT OF COLUMBIA
KENTUCKY
MARYLAND
MICHIGAN
NEW YORK
PENNSYLVANIA
VIRGINIA

WWW.WTPLAW.COM
(800) 987-8705

SUBMITTED VIA THE ONLINE PORTAL ONLY:
https://appengine.egov.com/apps/me/maine/ag/reportingform
Office of the Attorney General
Attorney General Aaron Frey

October 18, 2021

Re: Security Breach Notification

Dear Attorney General Frey,

We are writing on behalf of our client, Family of Woodstock, Inc. ("FOW") (located at P.O. Box 3516, Kingston, NY 12402), to notify you of a data security incident involving fourteen (14) Maine residents.

Nature

On August 3, 2021, FOW discovered that it was the victim of a sophisticated cyber incident. After discovering the incident, FOW quickly took steps to secure and safely restore its systems and operations. Further, FOW immediately engaged our firm and third-party forensic and incident response experts to conduct a thorough investigation of the incident's nature and scope and assist in the remediation efforts. FOW also contacted law enforcement, including both the local district attorney and the F.B.I. On September 11, 2021, FOW concluded its initial investigation and determined that the unauthorized individual likely gained access to its systems via a brute force attack.

Concurrently, FOW began a comprehensive review of the significant amount of stored data to determine the types of protected information that was exposed and identify individuals potentially impacted by the incident. On September 13, 2021, FOW concluded its initial review and determined that the incident potentially involved fourteen (14) Maine residents, and September 27, 2021, FOW located the most recent contact information for these individuals.

Regarding current or former patients, the protected health and personal information potentially impacted included demographic information (i.e., first and last names, addresses, telephone numbers, email addresses, dates of birth), social security numbers, driver's license numbers, medical information (i.e., medical record numbers, medical history, diagnosis, treatment, condition, or similar medical information), and health insurance information. Concerning current or former employees, the personal information included health insurance information, social security numbers, financial account numbers, and medical information.

However, as of now, FOW has no evidence of misuse of any of the potentially impacted information.

Notice and FOW's Response to the Event

On October 18, 2021, FOW will mail a written notification to the potentially affected Maine residents, pursuant to 45 CFR §§ 164.400-414 and 10 M.R.S.A. §§1346-1350-B, in a substantially similar form as the enclosed letter (attached as Exhibit A).

Additionally, FOW is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through Experian;
- Guidance on ways to protect against identity theft and fraud, including steps to report any suspected activities or events of identity theft or fraud to their credit card company and/or bank;
- The appropriate contact information for the consumer reporting agencies along with information on how to obtain a free credit report and place a fraud alert and security freeze on their credit file;
- 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 and law enforcement to report attempted or actual identity theft and fraud.

Further, FOW provided substitute notice via prominent media outlets and posted the notice to its website along with notifying the three major credit reporting agencies and the applicable government regulators, officials, and other state Attorneys General (as necessary).

Finally, FOW has implemented and continues to implement any necessary additional safeguards; enhance and improve its policies and procedures related to data protection; improve its cybersecurity infrastructure; and further train its employees on best practices to minimize the likelihood of this type of incident occurring again.

Contact Information

If you have any questions or wish to discuss this event further, please do not hesitate to call me on my direct dial (410) 832-8002 or email me at spollock@wtplaw.com.

Sincerely Yours,

Spencer S. Pollock, Esq., CIPP/US, CIPM

EXHIBIT A

Family of Woodstock
P.O. Box 3923
Syracuse, NY 13220

FAMILY
Family of Woodstock, Inc.
P.O. 3516
Kingston, NY 12402

[redacted]

October 18, 2021

Re: Notice of Data Breach

Dear [redacted]

At Family of Woodstock, Inc., we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your protected health or personal information, what we did in response, and steps you can take to protect yourself against possible misuse of this information.

What Happened

On August 3, 2021, we were the victim of a sophisticated cyber incident that impacted our networks and servers. After discovering the incident, we quickly took steps to secure our systems and restore operations. Further, we immediately engaged third-party incident response and forensic experts to conduct a thorough investigation of the incident's nature and scope and contacted the DA and the FBI to seek assistance and guidance. On September 11, 2021, we concluded our initial investigation and determined that the unauthorized individual gained access the same day we discovered the incident and potentially obtained information from our systems and servers.

At that time, we began a comprehensive review of the potentially impacted information. On September 13, 2021, we discovered that the incident potentially involved your protected health or personal information. ***As of now, we have no evidence indicating misuse of any of your information***. However, we wanted to notify you of the incident out of an abundance of caution and pursuant to our obligations under the Health Insurance Portability and Accountability Act (HIPAA).

What Information Was Involved

The protected personal information could potentially involve your demographic information (i.e., first and last name, address, telephone number (if you provided it us), email address (if you provided it us), or other similar demographic information if you provided it), <personal information>.

What We Are Doing

As explained above, we took immediate steps to secure our systems, filed a report with the DA and the FBI, and engaged third-party forensic experts to assist in the investigation. Further, in response to this incident, we are implementing additional cybersecurity safeguards, enhancing our employee cybersecurity training, and improving our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

The security and privacy of the information contained within our systems is a top priority for us. Therefore, while we have no evidence indicating your information was misused, we strongly recommend that you remain vigilant, monitor and review all of your financial and account statements, and report any unusual activity to the institution that issued the record and law enforcement. In addition, please see "other important information" on the following pages for guidance on how to best protect your identity.

Finally, we are providing you with access to Single Bureau Credit Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to your Experian credit file. This notification is sent to you the same day that the change or update takes place with the bureau. In addition, we are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a company specializing in fraud assistance and remediation services.

To enroll in Credit Monitoring* services at no charge, please log on to www.myidmanager.com and follow the instructions provided. When prompted please provide the following unique code to receive services:
[redacted]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

For More Information

We sincerely regret this incident occurred and for any concern it may cause. We understand that you may have questions about it beyond what is covered in this letter. If you have additional questions, please call our toll-free response line at 1-800-405-6108 Mondays through Fridays between 8:00 a.m. to 8:00 p.m. (EST). Representatives are available for 90 days from the date of this letter.

Sincerely yours,

Michael Berg, Executive Director

* Services marked with an "*" require an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report. We recommend that you obtain a free copy of your credit report from each of the three nationwide credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 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 can access the request form at https://www.annualcreditreport.com/requestReport/requestForm.action

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. The three nationwide credit reporting agencies' contact information are provided below to request a copy of your credit report or general identified above inquiries.

Equifax	**Experian**	**TransUnion**
(888) 766-0008	**(888) 397-3742**	**(800) 680-7289**
P.O. Box 740256	P.O. Box 2104	P.O. Box 6790
Atlanta, GA 30374	Allen, TX 75013	Fullerton, CA 92834
www.equifax.com	www.experian.com	www.transunion.com

Security Freeze (also known as a Credit Freeze). Following is general information about how to request a security freeze from the three credit reporting agencies. While we believe this information is accurate, you should contact each agency for the most accurate and up-to-date information. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. In addition, in some states, the agency cannot charge you to place, lift or remove a security freeze. There might be additional information required, and as such, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above).

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 https://www.equifax.com/personal/credit-report-services/credit-freeze/	**Experian Security Freeze** P.O. Box 9554 Allen, TX 75013 www.experian.com/freeze	**TransUnion** **Security Freeze & Fraud Victim Assistance Dept.** P.O. Box 6790 Fullerton, CA 92834 https://www.transunion.com/credit-freeze

Consider Placing a Fraud Alert on Your Credit Report. 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 twelve months. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting agencies identified above. Additional information is available at https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/

Remain Vigilant, Review Your Account Statements and Notify Law Enforcement of Suspicious Activity. As a precautionary measure, we recommend that you remain vigilant by closely reviewing your account statements and credit reports. If you detect any suspicious activity on an account, we strongly advise that you promptly notify the financial institution or company that maintains the account. Further, you should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). To file a complaint or to contact the FTC, you can (1) send a letter to the *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement agencies.

Take Advantage of Additional Free Resources on Identity Theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at https://www.consumer.ftc.gov/topics/privacy-identity-online-security. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). In addition, a copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf 0009_identitytheft_a_recovery_plan.pdf.

Maryland residents may wish to review the information the Attorney General, who can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, or visiting www.oag.state.md.us. **New Hampshire residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above. **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. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf **New York Residents**: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information: *New York Attorney General's Office Bureau of Internet and Technology*, (212) 416-8433, https://ag.ny.gov/internet/resource-center and or NYS Department of State's Division of Consumer Protection, (800) 697-1220, https://www.dos.ny.gov/consumerprotection. **North Carolina residents** may wish to review the information provided by the North Carolina Attorney General at www.ncdoj.gov, or by contacting the Attorney General by calling 877-5-NO-SCAM (Toll-free within North Carolina) or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office, Consumer Protection Division,* 9001 Mail Service Center Raleigh, NC 27699. **Oregon Residents**: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us. **Rhode Island residents** have the right to obtain a police report (if one was filed. 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. **West Virginia residents** have the right to ask that the three nationwide credit reporting agencies place fraud alerts in their file (as described above) and or request a security freeze (as described above). To place or fraud alert on your file or request the security freeze, please contact three credit reporting agencies identified above.