

June 5, 2024

Via Online Portal

**Attorney General Aaron Frey**

Office of the Attorney General

6 State House Station

Augusta, ME 04333

**Re: Our Client : Family Health Center**  
**: Data Security Incident on January 25, 2024**  
**Wilson Elser File No. : 15991.01720**

---

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Family Health Center (hereinafter, “FHC”), located at 117 W. Paterson Street, Kalamazoo, MI 49007 with respect to a data security incident that it experienced. This letter will serve to inform you of the nature of the incident, what information may have been compromised, the number of individuals being notified, and the steps that FHC has taken in response to the Incident.

### **1. Nature of the Incident**

On January 25, 2024, FHC experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, FHC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that there is evidence to suggest some of FHC files were accessed by an unauthorized actor. Upon learning of this, FHC began an extensive and comprehensive review to identify impacted individuals and any sensitive information involved. On May 30, 2024, FHC finalized the list of individuals to notify and identified their addresses to the extent available.

As of this writing, FHC has not received any reports of any related identity theft since the date of the incident (January 25, 2024, to present).

### **2. What Information Was Involved?**

Based on the investigation, employees may have name, address, health insurance information, and Social Security Number impacted.

In regards to patients, the information varied by individuals. The following information may have been subject to unauthorized access: first name; last name; and medical information. Social Security Numbers were not impacted.

---

55 West Monroe Street, Suite 3800 • Chicago, IL 60603 • p 312.704.0550 • f 312.704.1522

Alabama • Albany • Atlanta • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston  
Indiana • Kentucky • Las Vegas • London • Los Angeles • Miami • Michigan • Milwaukee • Mississippi • Missouri • Nashville • New Jersey • New Orleans  
New York • Orlando • Philadelphia • Phoenix • San Diego • San Francisco • Sarasota • Stamford • Virginia • Washington, DC • Wellington • White Plains

**wilsonelser.com**

**3. Number of Maine Residents Notified.**

A total of three (3) residents of Maine were potentially affected by this security incident. These individuals are current and former employees or patients of FHC. A sample copy of the notification letter is included with this letter under **Exhibit A**.

**4. Steps taken in response to the Incident.**

Data privacy and security is among FHC's highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, FHC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, FHC engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, FHC took the following steps, including, but not limited to: increasing data access control measures, expanding multi-factor authentication and other security measures, and increasing monitoring for suspicious activities. FHC will continue to take steps to mitigate the risk of future harms.

Although FHC is not aware of any evidence of misuse of personal information, FHC extended to all potentially an offer for free credit monitoring and identity theft protection through Cyberscout. This service will include 12 months of credit monitoring, along with a fully managed identity theft recovery service, should the need arise.

**5. Contact information**

If you have any questions or need additional information, please do not hesitate to contact Joseph M. Fusz at [Joseph.Fusz@wilsonelser.com](mailto:Joseph.Fusz@wilsonelser.com) or 312-821-6141.

Very truly yours,

**Wilson Elser Moskowitz Edelman & Dicker LLP**



Joseph M. Fusz

Enclosures: *Sample Notification Letter*

# **EXHIBIT A**

Family Health Center  
c/o Cyberscout  
PO Box 1286  
Dearborn, MI 48120-9998




**FAMILYHEALTH**  
**center**

MOSES L. WALKER BUILDING  
117 W. PATERSON ST, KALAMAZOO, MI 49007  
T (269) 349-2641 U WWW.FHCKZOO.COM



*Via First-Class Mail*

**Re: Notice of Data Security Incident**

Dear ,


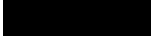
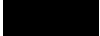



Family Health Center (“FHC”) is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. While we are unaware of any fraudulent misuse of your personal information at this time, we are providing you with details about the incident, steps we are taking in response, and resources available to help you protect against the potential misuse of your information.

**What Happened?**

On January 25, 2024, FHC experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, FHC immediately disconnected all access to the network and promptly engaged a specialized third-party cybersecurity firm and IT personnel to assist with securing the environment, as well as, to conduct a comprehensive forensic investigation to determine the nature and scope of the incident. The forensics investigation determined that there is evidence to suggest some of FHC files were accessed by an unauthorized actor.

Based on the findings of the forensic investigation, FHC began an extensive and comprehensive review of the potentially affected files to identify what information was impacted. This review identified that some of your personal information may have been impacted by this incident. On May 28, 2024, FHC finalized the list of individuals to notify and identified their addresses to the extent available.

**What Information Was Involved?**

Although FHC has no evidence that any sensitive information has been misused by third parties as a result of this incident, we are notifying you out of an abundance of caution and for purposes of full transparency. Based on the investigation, the following information related to you may have been subject to unauthorized access:   
 and  Your    was not impacted as a result of this incident.

**What We Are Doing**

Data privacy and security is among FHC’s highest priorities, and we are committed to doing everything we can to protect the privacy and security of the personal information in our care. Upon discovery of the Incident, FHC moved quickly to investigate and respond to the Incident and assessed the security of its systems. Specifically, FHC engaged a specialized cybersecurity firm and IT personnel to conduct a forensic investigation to determine the nature and scope of the Incident.

0000102G0400

P

Additionally, FHC took the following steps, including, but not limited to: increasing data access control measures, expanding multi-factor authentication and other security measures, and increasing monitoring for suspicious activities. FHC will continue to take steps to mitigate the risk of future harm.

In light of the incident, we are also providing you with [REDACTED] months of complimentary credit monitoring and identity theft restoration services through Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, you will need to complete the activation process by following the instructions below.

### **What You Can Do**

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious or unauthorized activity. Additionally, security experts suggest that you contact your financial institution and all major credit bureaus to inform them of such a breach and then take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on your credit file. Please review the enclosed *Steps You Can Take to Help Protect Your Information*, to learn more about how to protect against the possibility of information misuse.

You may also activate the credit monitoring services we are making available to you at no cost. The deadline to enroll is 08/31/2024.

To enroll in Credit Monitoring services at no charge, please log on to <https://bfs.cyberscout.com/activate> 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. The enrollment requires 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.

We would like to reiterate that, at this time, there is no evidence that your information was misused. However, we encourage you to take full advantage of the services offered.

### **For More Information**

If you have any questions or concerns not addressed in this letter, please call our dedicated assistance line at **833-566-9936** Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

FHC sincerely regrets any concern or inconvenience this matter may cause and remains dedicated to ensuring the privacy and security of all information in our control.

Sincerely,

Denise Crawford

*Denise Crawford*

President & Chief Executive Officer  
Family Health Center

## Steps You Can Take to Help Protect Your Information

**Credit Reports:** You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com), or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

**Fraud Alerts:** You can place fraud alerts with the three credit bureaus by phone or online. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years.

### Experian

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

### TransUnion

P.O. Box 2000  
Chester, PA 19016  
1-800-680-7289

### Equifax

P.O. Box 105069  
Atlanta, GA 30348  
1-800-525-6285

[www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html) [www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts) <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

**Monitoring:** You should always remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and by monitoring your credit report for suspicious or unusual activity.

**Security Freeze:** You have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

### Experian

P.O. Box 9554  
Allen, TX 75013  
1-888-397-3742

### TransUnion

P.O. Box 160  
Woodlyn, PA 19094  
1-888-909-8872

### Equifax

P.O. Box 105788  
Atlanta, GA 30348-5788  
1-888-298-0045

[www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html) [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze) <https://www.equifax.com/personal/credit-report-services/credit-freeze/>

**File Police Report:** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.



**FTC and Attorneys General:** You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338), 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. You can obtain further information on how to file such a complaint by way of the contact information listed above. Instances of known or suspected identity theft should also be reported to law enforcement.

---

**For residents of Iowa:** State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

---

**For residents of Massachusetts:** It is required by state law that you are informed of your right to obtain a police report filed 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.

---

**For residents of New Mexico:** State law advises you to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. 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 reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You 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 you to review your rights pursuant to the Fair Credit Reporting Act at [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://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 residents of Oregon:** State law advises you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

---

**For residents of Rhode Island:** It is required by state law that you are informed of your right to file or obtain a police report in regard to this incident.

---

**For residents of Arizona, Colorado, District of Columbia, Illinois, Maryland, New York, North Carolina, and Rhode Island:** You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

**Federal Trade Commission** - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); [www.identitytheft.gov](http://www.identitytheft.gov)

**Arizona Office of the Attorney General** Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025

**Colorado Office of the Attorney General** Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 [www.coag.gov](http://www.coag.gov)

**District of Columbia Office of the Attorney General** - Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; [www.oag.dc.gov](http://www.oag.dc.gov)

**Illinois office of the Attorney General** - 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; [www.illinoisattorneygeneral.gov](http://www.illinoisattorneygeneral.gov)

**Maryland Office of the Attorney General** - Consumer Protection Division: 200 St. Paul Place, 16<sup>th</sup> floor, Baltimore, MD 21202; 1-888-743-0023; [www.oag.state.md.us](http://www.oag.state.md.us)

**New York Office of Attorney General** - Consumer Frauds & Protection: The Capitol, Albany, NY 12224; 1-800-771-7755; <https://ag.ny.gov/consumer-frauds/identity-theft>

**North Carolina Office of the Attorney General** - Consumer Protection Division: 9001 Mail Service Center, Raleigh, NC 27699; 1-877-566-7226; [www.ncdoj.com](http://www.ncdoj.com)

**Rhode Island Office of the Attorney General** - Consumer Protection: 150 South Main St., Providence RI 02903; 1-401-274-4400; [www.riag.ri.gov](http://www.riag.ri.gov)