Kennedys

1600 Market Street
Suite 1410
Philadelphia, PA 19103
USA

t +1 267.951.7196
f +1 215.665.8475

kennedyslaw.com

t +1 267 951.7196
Matthew.Smith@kennedyslaw.com
March 27, 2026

By Webform

Attorney General Aaron Frey
Maine Office of Attorney General
Consumer Protection Division
6 State House Station
Augusta, Maine 04333

Re: Notice of Data Incident

Dear Attorney General Frey:

We write on behalf of our client Woodfords Family Services ("Woodfords") to notify your office of a data breach pursuant to M.E. STAT. ANN. T. 10 § 1346. Woodfords is a provider of specialized clinical, educational and behavioral services for individuals with disabilities based in Westbrook, Maine. The incident involved the personal identifiable information of 7,7701 residents of Maine[1]. This notice may be supplemented with new information learned after submission.

On April 8, 2024, Woodfords discovered suspicious activity within its network that ultimately was a ransomware event caused by the actor group Medusa. Upon discovery, Woodfords took immediate action to secure its network and to address and investigate the incident. This included retaining our office, and we retained forensic specialists to investigate the incident. The investigation determined that Woodfords' systems were subject to unauthorized access on April 8, 2024, and it identified data staging and activities typically associated with data exfiltration. The forensic investigation ended on May 30, 2024.

Woodfords then began an internal review process to identify the scope of potentially impacted data and to whom it belonged. It was anticipated that this matter was solely governed

[1] 3,695 of these individuals are nonresidents of Woodfords. 4,006 of these individuals are current or former Woodfords residents who were notified pursuant to the Health Insurance Portability and Accountability Act. In addition, Woodfords is posting on its website substitute notice under HIPAA and noting PII involved for persons whose address Woodfords does not have.

Kennedys is a trading name of Kennedys CMK LLP. Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

Kennedys offices, associations and cooperations: Argentina, Australia, Belgium, Bermuda, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Portugal, Puerto Rico, Russian Federation, Scotland, Singapore, Spain, Sweden, Thailand, United Arab Emirates, United States of America.

under HIPAA. Out of an abundance of caution, on June 3, 2024, Woodfords submitted a preliminary notice of this incident to the Department of Health and Human Services, Office for Civil Rights. Media notice was also submitted on June 7, 2024, to make individuals aware of the incident as soon as possible while the data review was ongoing.

Woodfords ultimately determined they could not identify the full scope of this incident internally, and data mining specialists were engaged on September 25, 2024 to confirm the scope of information involved and to whom the information belonged. This resulted in an extensive, comprehensive review process. The initial data mining process concluded on October 3, 2025. However, the data population required further internal review to identify whether any involved individuals were not governed under HIPAA. On January 29, 2026, Woodfords learned that the involved population included the personally identifiable information of 3,695 Maine residents, in addition to 4,007 Maine residents to be notified pursuant to HIPAA. This included first and last names along with Social Security numbers, driver's license numbers, financial account information, medical diagnostic and treatment information, and health insurance information. Woodfords then engaged in additional address look-ups to ensure the correct contact information for involved individuals.

Woodfords notified these individuals via First Class U.S. mail on March 27, 2026. Woodfords is offering 12 months of single bureau credit monitoring, fraud consultation, and identity theft restoration services through Cyberscout, a TransUnion company, to individuals whose Social Security numbers were included in the impacted data set. Woodfords has set up a professional call center to respond to individuals' inquiries and to assist with fraud consultation resources and credit monitoring enrollment. A sample copy of the notification letter is enclosed. Woodfords also is reviewing its existing security policies and protections previously in place on its network and adopting additional security to safeguard against evolving threats moving forward. Woodfords is notifying the three major credit reporting bureaus Experian, Equifax, and TransUnion, and as noted, has also notified the Department of Health and Human Services, Office for Civil Rights of this incident.

Should you have any further questions at this stage, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/ Matthew C. Smith

Matthew C. Smith
Associate
for Kennedys

Enclosures: Sample Consumer Notification Letter

cc: Joshua A. Mooney, Esquire (joshua.mooney@kennedyslaw.com)

[redacted]

Woodfords Family Services
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

[redacted]

March [redacted] 2026

NOTICE OF DATA SECURITY INCIDENT

Dear [redacted]:

Woodfords Family Services takes the privacy and security of your personal information seriously. As part of that commitment, we write to notify you of a data privacy incident involving your personal information. This notice explains the incident, our response, and steps one may take for added protection of personal information, if desired. We are also offering the opportunity to enroll in complimentary credit monitoring and identity protection services.

What Happened? On April 8, 2024, we discovered suspicious activity within our network. We took steps to secure our environment and forensic specialists were engaged to investigate and understand the nature and scope of the disruption. Our investigation determined that certain files and folders from our network were subject to unauthorized access that same day. Out of an abundance of caution, we then began a comprehensive review of these files and folders and we determined that your personal information as described below, was involved.

What Information Was Involved? The information involved included your name in combination [redacted].

What We Are Doing. We have no indication of fraud or identity theft occurring as a result of this incident. Upon learning of the incident, we took immediate steps to address it, including securing our systems and taking parts of our network offline. Forensic specialists were engaged, and we notified federal law enforcement.

We also are offering you access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for [redacted] months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you discovery suspicious activity. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. Instructions for how to enroll in these services are enclosed.

What You Can Do. As a general matter, it is best practice to remain vigilant for incidents of identity theft and fraud from any source by reviewing your credit reports and account statements for suspicious activity and errors. If you discover any suspicious or unusual activity on your accounts, promptly contact your financial institution or service provider. Please refer to the enclosed "*Steps You Can Take to Help Protect Your Information*" for additional resources to protect against fraud and identity theft, should you feel it appropriate to do so.

For More Information. Should you have any questions or concerns, please contact our assistance line at 1-833-877-8966, Monday through Friday 8:00am - 8:00pm Eastern Time, excluding major U.S. holidays. We take this incident very seriously and sincerely regret any inconvenience or concern this incident may cause you.

P 0000101102G0400

[redacted]

Sincerely,

Woodfords Family Services

Enclosure: *Steps You Can Take to Help Protect Your Information*

[redacted]

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

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.



P 00001020280000

Monitor Your Accounts and Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You 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, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you 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 your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

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

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

TransUnion 1-800-680-7289 www.transunion.com **TransUnion Fraud Alert** P.O. Box 2000 Chester, PA 19016-2000 **TransUnion Credit Freeze** P.O. Box 160 Woodlyn, PA 19094	**Experian** 1-888-397-3742 www.experian.com **Experian Fraud Alert** P.O. Box 9554 Allen, TX 75013 **Experian Credit Freeze** P.O. Box 9554 Allen, TX 75013	**Equifax** 1-888-298-0045 www.equifax.com **Equifax Fraud Alert** P.O. Box 105069 Atlanta, GA 30348-5069 **Equifax Credit Freeze** P.O. Box 105788 Atlanta, GA 30348-5788

[redacted]

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

This notice has not been delayed by law enforcement.

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

For Maryland Residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

For Iowa residents, the Iowa Attorney General may be contacted at 1305 E. Walnut Street, Des Moise, IA 50419; 1-515-281-5164; and iowaattorneygeneral.gov.

For Maryland residents, the Maryland Attorney General may be contacted at 200 St, Paul Place, Baltimore, MD 21202; 1-410-576-6300; and marylandattorneygeneral.gov.

For Massachusetts residents, the Massachusetts Attorney General may be contacted at 1 Ashburton Place, 20th Floor, Boston, MA 02108; 1-617-727-8400 or 1-617-727-2200; and www.mass.gov/orgs/office-of-the-attorney-general.

For New Mexico Residents, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

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 Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and https://doj.state.or.us/consumer-protection/.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. [# of RI] residents had their data impacted by this incident.