

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

November 18, 2021

Re: Security Breach Notification

To Whom It May Concern:

We are writing on behalf of our client, Episcopal Retirement Services (“ERS”) (3870 Virginia Ave., Cincinnati, Ohio 45227), to notify you of a data security incident involving two (2) Maine residents.¹ ERS is a network of senior living communities and provides related services to seniors, including in-home and community-based services.

Nature

On or about September 24, 2021, ERS discovered that it was the victim of a cyberattack that impacted its systems and servers. After discovering the incident, ERS quickly took steps to secure and safely restore its systems and operations. However, on October 22, 2021, ERS experienced another incident which was ultimately determined to be a ransomware attack. At this time, ERS also learned that the September incident was a ransomware attack. ERS 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. ERS also contacted the FBI to report the incidents and seek guidance. The investigation is ongoing and, as of now, ERS has not determined how its systems were accessed.

Concurrently, ERS began a comprehensive review of a significant amount of stored data to determine the types of protected information that was potentially exposed and identify individuals potentially impacted by the incident. ERS concluded its initial review and determined that the incident potentially involved two (2) Maine residents. On November 16, 2021, ERS located the most recent contact information for these individuals.

The personal information potentially impacted included first and last names, addresses, gender, social security numbers, phone numbers, and dates of birth. The information potentially impacted also may have included medical diagnoses, health care provider name, insurance numbers, and Medicare number. However, as of the date of this letter, ERS has no evidence of misuse of any of the potentially impacted information.

¹ By providing this notice, ERS does not waive any rights or defenses regarding the applicability of Maine law, the applicability of the Maine data event notification statute, or personal jurisdiction.

Notice and ERS' Response to the Event

On November 19, 2021, ERS 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, ERS is providing the potentially impacted individuals the following:

- Free access to credit monitoring services for one year through Sontiq;
- 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, ERS notified the three major credit reporting agencies and applicable government regulators, officials, and Attorneys General (as necessary). Finally, ERS is working to implement additional safeguards to its existing cybersecurity infrastructure, enhancing employee cybersecurity training, and working to improve its cybersecurity policies, procedures and protocols to help 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

November 19, 2021



Re: Notice of Data Breach

Dear ,

At Episcopal Retirement Services, 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. The incident may involve your personal information. The following communication details, what we did in response to the incident, and the steps you can take to protect yourself against possible misuse of your personal information.

What Happened

On or about September 24, 2021, we discovered that we were the victim of a cyber-attack that impacted our systems and servers. At that time, our technology team acted quickly to restore and secure our systems. However, on October 22, 2021, we experienced a ransomware attack. At this time, we learned that the September incident was also a ransomware attack. We immediately engaged independent third-party cybersecurity experts to assist in the remediation and investigation and contacted the FBI. As you have likely seen on the news, we are one of thousands of organizations dealing with these types of incidents. We followed the guidance set forth by the FBI and are actively working on remediation and restoration of all our systems.

The investigation is ongoing, but we believe that the unauthorized individual could have potentially obtained or accessed your protected personal health information. As such, while we have not confirmed this fact, out of an abundance of caution, we are providing you with information about the steps you can take to help protect your identity. ***With this said, as of now, we have no evidence indicating that any of your personal information has been misused.***

What Information Was Involved

The types of protected health information potentially involved include your first and last name, address, name, gender, home address, phone number, date of birth, and social security number. It may also include your medical diagnosis, health care provider name, insurance numbers, and Medicare number.

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. In response to this incident, we are implementing additional safeguards to our existing cybersecurity infrastructure and enhancing our employee cybersecurity training. Further, we are working with our external legal and cybersecurity

experts to improve our cybersecurity policies, procedures, and protocols to help minimize the likelihood of this type of incident occurring again.

What You Can Do

As stated above, while we have no evidence indicating your information was misused, we strongly recommend 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.

Further, we are providing you with access to Single Bureau Credit Monitoring* for [REDACTED] years. These services provide you with alerts for [REDACTED] years from the date of enrollment when changes occur to your Experian credit file. We are providing this service free of charge, and signing up for this service will not impact your credit score. This product helps detect any potential misuse of your personal information and gives you identity protection services that will help with resolving and identifying any potential identity fraud or theft. These services will be provided by Sontiq, a company specializing in fraud assistance and remediation services.

To enroll in these services, please log on to [REDACTED] and follow the instructions provided. When prompted, please provide the following unique code to receive services: [REDACTED]

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, Monday through Friday between 8:00 a.m. and 8:00 p.m. (ET).

Sincerely yours,



Laura Lamb, President & CEO

* 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
(888) 766-0008
P.O. Box 740256
Atlanta, GA 30374
www.equifax.com

Experian
(888) 397-3742
P.O. Box 2104
Allen, TX 75013
www.experian.com

TransUnion
(800) 680-7289
P.O. Box 6790
Fullerton, CA 92834
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](https://www.ftc.gov/identity-theft) 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.

District of Columbia Residents: You can obtain information from the FTC and the Office of the Attorney General for the District of Columbia about steps to take to avoid identity theft. You can contact the D.C. Attorney General at 441 4th Street, NW, Washington, DC 20001, 202-727-3400, www.oag.dc.gov. **Iowa residents** may also wish to contact the Office of the Attorney general on how to avoid identity theft by calling 515-281-5164 or by mailing a letter to the Attorney General at *Office of the Attorney General of Iowa*, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319. **Maryland residents** may wish to review the Attorney General's information, 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. **Massachusetts residents:** State law advises you that you have the right to obtain a police report. You also will not be charged for seeking a security freeze, as described above in this document. **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. **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 <https://ncdoj.gov/protecting-consumers/identity-theft/>, or by contacting the Attorney General by calling 1-877-566-7226 or emailing or by mailing a letter to the Attorney General at *North Carolina Attorney General's Office* 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.