May 16, 2023

M. Mendel Epstein
212.915.5237 (direct)
Mendel.Epstein@wilsonelser.com

Via Online Submission

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Re: Notice of Cybersecurity Incident

To Whom It May Concern:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Bay Shore Brightwaters Rescue Ambulance, Inc. ("BSBRA"), an ambulance company located at 911 Aletta Pl #7940, Bay Shore, NY 11706, with respect to a cybersecurity incident that was confirmed by BSBRA on April 25, 2022 (hereinafter, the "Incident"). BSBRA takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the Incident

On or about April 25, 2022, BSBRA became aware of a compromise to its e-mail environment, which may have resulted in the inadvertent exposure of personal information. Upon discovery of the Incident, BSBRA worked diligently with a third-party forensic investigator to determine what happened and what information may have been involved as a result of this Incident. The results of the forensic investigation indicated that four (4) BSBRA volunteer e-mail user accounts may have been accessed by an unauthorized user.

Based upon the results of the forensic investigation, BSBRA initiated a review of the data maintained within the potentially compromised e-mail user accounts for purposes of providing notification to the affected individuals. On December 6, 2023, BSBRA mailed a first wave of notice letters to the individuals whose information was impacted as a result of the Incident. Upon further investigation, BSBRA discovered on March 8, 2023, that additional sensitive personal information was impacted as a result of the Incident. Based upon the subsequent review, on April 5, 2023, BSBRA distributed a second wave of notification letters to the affected individuals. On April 10, 2023, BSBRA initiated a third and final review of the compromised e-mail accounts, which concluded on April 27, 2023. The results of the final review indicated that a limited number of additional personal information w impacted as a result of the Incident. Based upon these results, BSBRA distributed a third wave of notification letters the affected Individuals.

During its most recent and final investigation, BSBRA determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: full names, addresses, dates of births, drivers' license numbers, Social Security numbers, account access information, limited financial information, limited treatment and diagnostic information, limited health insurance information, health provider information, limited prescription information, and incidental health information. The exact elements of personal information that may have been exposed as a result of this Incident varies per individual.

As of this writing, BSBRA has completed its review of the compromised e-mail user accounts. In addition, BSBRA has not received any reports to date of misuse of any personal information resulting from this Incident.

2. Number of Maine residents affected.

During its third and final review of the compromised e-mail user accounts, BSBRA discovered that the Incident may have resulted in unauthorized exposure of information pertaining to one (1) Maine resident. A notification letter to this individual was mailed on May 15, 2023, by First Class Mail. A sample copy of the notification letter is included with this letter as **Exhibit A**.

3. Steps taken in response to the Incident.

BSBRA is committed to ensuring the security and privacy of all personal information in its control, and is taking steps to prevent a similar incident from occurring in the future. Upon discovery of the Incident, BSBRA moved quickly to investigate and respond to the Incident. Specifically, BSBRA engaged a specialized cybersecurity firm to conduct a forensic investigation to determine the nature and scope of the Incident. Additionally, BSBRA is taking steps to strengthen its security posture to prevent a similar event from occurring again in the future.

BSBRA is also offering twelve (12) months of complimentary credit monitoring and identity theft restoration services through Cyberscout to all individuals to help protect their identity. Additionally, BSBRA provided guidance on how to better protect against identity theft and fraud, including providing information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and the contact details for the Federal Trade Commission.

4. Contact information

BSBRA remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at mendel.epstein@wilsonelser.com or 212-915-5237.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Mendel Epstein

M. Mendel Epstein

EXHIBIT A

Bay Shore Brightwaters Rescue Ambulance, Inc.
P.O. Box 3923
Syracuse, NY 13220

Via First-Class Mail

To Enroll, Please Visit:
https://secure.identityforce.com/benefit/bayshore
Membership Number:
[redacted]

[redacted]

May 15, 2023

Notice of Data Incident

Dear [redacted]:

Bay Shore Brightwaters Rescue Ambulance, Inc. ("BSBRA") is writing to notify you that it experienced a data security incident which may have affected your personal information (the "Incident"). Please note we take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this Incident may cause. This notice contains additional information about the Incident, our response to this Incident, and steps you can take to protect your information.

What Happened

On or about April 25, 2022, BSBRA discovered a compromise to its e-mail environment, which may have resulted in the inadvertent exposure of personal information. We have since worked diligently with a third-party forensic investigator to determine what happened and what information was involved as a result of this Incident. The forensic investigation concluded that between February 16, 2022 and February 22, 2022, BSBRA's e-mail tenant was accessed by an unauthorized user.

Based upon the results of the forensic investigation, BSBRA initiated a review of the information maintained within the compromised e-mail accounts for purposes of providing notice to the individuals whose information was impacted as a result of the Incident. On July 28, 2022, BSBRA concluded its initial review of the compromised email accounts. Based upon the results of its initial review, on December 6, 2022, BSBRA mailed a first wave of notice letters to the individuals whose information was impacted as a result of the Incident. Upon further investigation, BSBRA discovered on March 8, 2023, that additional health information was impacted as a result of the Incident. Based upon the results of its subsequent review, on April 5, 2023, BSBRA mailed a second wave of notice letters to the individuals whose information was impacted as a result of the Incident.

On April 10, 2023, BSBRA conducted a third and final review of the compromised e-mail accounts, which concluded on April 27, 2023. The results of the final review indicated that a limited number of additional individuals' personal information may have been impacted as a result of the incident. Based upon these results, BSBRA is notifying the additional individuals whose information may have been impacted as a result of the Incident. At this time, BSBRA has completed its review of the compromised e-mail user accounts.

What Information Was Involved

The elements of your personal information that may have been exposed may have included, and potentially were not limited to your: **Date of Birth, and Social Security Number**. Please note that there is no evidence at this time that any of your personal information has been misused as a result of this Incident.

What We Are Doing

We are working with cybersecurity experts to determine the necessary actions in responding to the Incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to strengthen our security posture to prevent a similar event from occurring again in the future.

As a safeguard, we are providing you with 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 twelve 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 become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To enroll in this service, please log on to https://secure.identityforce.com/benefit/bayshore and follow the instructions provided. When prompted please provide the following unique code to receive services: [redacted]**.** Please see more information regarding the enrollment process at the end of this letter.

What You Can Do

You can sign up for the credit monitoring service within ninety (90) days of the date of this letter. Please note that when signing up for credit monitoring services, you may be asked to verify personal information to confirm your identity. Enrollment for credit monitoring services requires an internet connection and e-mail account, and might not be available for individuals under the age of eighteen (18). Enrolling in this service will not affect your credit score.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. Representatives are available for ninety (90) days from the date of this letter, to assist you with questions regarding this Incident. If you have any questions, please do not hesitate to call 1-800-405-6108 Monday – Friday, 8:00 am to 8:00 pm Eastern Time.

Sincerely,

Bay Shore Brightwaters Rescue Ambulance, Inc.

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois*, *Iowa*, *Maryland*, *Missouri*, *North Carolina*, *Oregon*, and *West Virginia*:
It is required by state laws to inform you that 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, 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.

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 *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

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

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

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

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion(https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). 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. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also 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:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
https://www.equifax.com/personal/credit-report-services/credit-freeze/	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

Free Credit Report Information: Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.
If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Get a copy of the report; many creditors want the information it contains to absolve you of the fraudulent debts. You also should file a complaint with the Federal Trade Commission (FTC) at www.identitytheft.gov or at 1-877-ID-THEFT (1-877- 438-4338). Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcers for their investigations. Also visit the FTC's website at www.ftc.gov/idtheft to review their free identity theft resources such as their comprehensive step-by-step guide "Identity Theft - A Recovery Plan".