



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

November 22, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Supplemental Notice of Data Event

To Whom It May Concern:

As you know, we represent Superior Air-Ground Ambulance Service, Inc., located at 395 W. Lake St., Elmhurst, Illinois 60126, and are writing to supplement our September 3, 2024 notice of a data event to your office. Superior is providing this supplemental notice on behalf of itself and relevant affiliated covered entities and subsidiaries, including Metro Paramedic Services, Inc. and Illinois Medi-Car, Inc., and Paramedic Billing Services, Inc. (collectively, "Superior"). This notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Superior does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

As provided in our September 3, 2024 notification to your Office, in late May 2023, Superior learned of unusual activity within its computer systems, and quickly worked to secure the systems and complete a comprehensive investigation to confirm the full nature, scope, and impact of the event. On June 23, 2023, the investigation determined that an unauthorized actor may have viewed and/or copied certain files on computer systems between May 17 and May 23, 2023. While its investigation was ongoing and prior to determined specific individuals that may be affected, based on a preliminary assessment that the information in the affected files was likely related to Paramedic Billing Services, Inc., Superior began providing notice via website posting of the event

on or about July 21, 2023. Notice was also provided to the U.S. Department of Health and Human Services (“HHS”).

Subsequently, Superior undertook a comprehensive review of the relevant files to determine specifically what information was present in the affected files and to whom the information relates. This process involved working with third-party data review specialists to complete a review and cataloging of the affected files, and then a comprehensive reconciliation of the resulting data list with internal records to identify what information may be affected, to whom that information belonged, and contact information for potentially affected individuals. While these efforts were ongoing, through this review, it was confirmed in February 2024 that, in addition to Paramedic Billing Services, Inc. the affected files also contained information relating to the aforementioned Superior entities. Beginning on May 10, 2024, Superior provided notice of this event on its respective websites and to prominent media outlets in relevant jurisdictions. Superior also provided notification to affected data owners and submitted additional notification to HHS. As Superior worked to complete its investigation and coordinating with relevant data owners, based on its exhaustive data review and reconciliation efforts, Superior provided written notification to affected individuals via mail on September 3, 2024. Superior recently completed its investigation and is now providing notice via mail to remaining affected individuals.

The information that could have been subject to unauthorized access includes name, Social Security number, health insurance information, medical information, and financial account information.

Notice to Maryland Residents

Superior previously provided written notification of this incident to affected [State] residents on September 3, 2024. On or about November 22, 2024, Superior is subsequently providing written notice of this incident to an additional eleven (11) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Superior has undertaken extensive efforts to investigate this incident and determine what information may be affected. Further, Superior notified federal law enforcement regarding the event. Superior has implemented enhanced technical safeguards and reviewed its policies and procedures. Additionally, Superior has and is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with 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 encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Superior is also providing individuals with Social Security number affected with access to credit monitoring services for twelve (12) months, through TransUnion at no cost to these individuals. Superior is providing written notice of this event to relevant state and

Office of the Attorney General

November 22, 2024

Page 3

federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion. As discussed above, Superior has also notified HHS and prominent media outlets pursuant to HIPAA.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,

M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/dle
Enclosure

EXHIBIT A

Superior Air-Ground Ambulance Service, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



November 22, 2024

Re: Notice of Data Event

Dear _____ :

Superior Air-Ground Ambulance Service, Inc., on behalf of itself and relevant affiliated covered entities and subsidiaries, including Metro Paramedic Services, Inc. and Illinois Medi-Car, Inc., (“Superior”), is writing to inform you of an incident that may affect your information. This letter provides you with information about the incident, our response to it, and steps you can take to help protect your personal information, should you feel it appropriate to do so.

What Happened? In May 2023, Superior learned of unusual activity within its computer systems. We promptly took steps to secure the system and began a comprehensive investigation to confirm the full nature, scope, and impact of the event. On June 23, 2023, the investigation determined that an unauthorized actor copied certain files from the network between May 15 and May 23, 2023. We subsequently worked to undertake a comprehensive and time-intensive review of the affected files to identify and catalogue what information was present and to whom that information relates. We then worked to determine contact information for those individuals. You are receiving this notice because we determined that some of your information was present in the relevant files.

What Information Was Involved? Based on the investigation, the potentially impacted data varied from individual to individual, but we determined that your _____ may be affected.

What We Are Doing. We view our responsibility to safeguard information in our possession as an utmost priority. Upon learning of this incident, we promptly took steps to secure the system and began a comprehensive investigation. We have been working diligently to provide affected individuals with accurate and complete notice. We have taken steps to review our policies and procedures and have implemented additional security measures. We are also providing notice of this incident to potentially impacted individuals and providing you with guidance on how to better protect your information, should you feel it is appropriate to do so. We have also notified relevant state and federal regulators as applicable.

Out of an abundance of caution, 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 (12) 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 the event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services. While we are covering the cost of these services, due to privacy restrictions, you will need to complete the activation process yourself. Information on enrollment is in the enclosed *Steps You Can Take to Protect Personal Information*.

000010102G0400

P

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You can also find out more about how to safeguard your information in the enclosed *Steps You Can Take to Protect Personal Information*.

For More Information. If you have questions about this incident, please call our dedicated assistance line at 1-833-566-2450, 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays. Individuals may also write to Superior directly at 395 W. Lake Street Elmhurst, IL 60126, Attn: Legal Department.

Sincerely,

Superior Air-Ground Ambulance Service, Inc.

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

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

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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094



Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting 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 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 Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately 0 Rhode Island residents that may be impacted by this event.