April 14, 2025

Joseph M. Fusz
312.821.6164 (direct)
joseph.fusz@wilsonelser.com

Via Online Portal

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

Re: Cybersecurity Incident Involving Medical Express Ambulance Inc. D/B/A MedEx Ambulance

Dear Attorney General Frey:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Medical Express Ambulance Inc. D/B/A MedEx Ambulance ("MedEx") an ambulance service provider located at 5650 W Howard Street Skokie, IL 60077 with respect to a recent cybersecurity incident that was first discovered by MedEx on March 18, 2024 (hereinafter, the "Incident"). MedEx takes the security and privacy of the information in its control very seriously and has taken steps to prevent a similar incident from occurring in the future.

This letter will serve to inform you of the nature of the Incident, what information may have been compromised, the number of Maine residents being notified, and the steps that MedEx has taken in response to the Incident. We have also enclosed hereto a sample of the notification made to the potentially impacted individuals, which includes an offer of free credit monitoring services.

1. Nature of the Incident

On March 18, 2024, MedEx experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, MedEx 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 forensic investigation determined that that personal information may have been acquired by the threat actor.

Based on these findings, MedEx decided to proceed with an analysis of the compromised data for any potential sensitive personal information ("PII") or protected health information ("PHI"). MedEx engaged a third-party vendor to review the data that was compromised. The data mining process took some time given the complexities of the types and the volume of the data analyzed, requiring multiple phases of automated and manual review. Data mining was completed on January 30, 2025. On March 3, 2025, MedEx engaged a third-party notice vendor to assist with

the mailings, call center, and provide identity theft protection services. Thereafter, MedEx worked to verify the patient information and addresses for mailing. On March 19, 2025, MedEx finalized the list of individuals to notify.

Although MedEx is unaware of any fraudulent misuse of information, it is possible that individuals' full name; date of birth; demographic information, Social Security number, driver's license number; medical information; financial information; and health insurance information, username and password; and for some passport may have been exposed as a result of this unauthorized activity.

As of this writing, MedEx has not received any reports of related identity theft since the date of the incident (March 18, 2024, to present).

2. Number of Maine residents affected.

MedEx identified and notified 118,418 individuals potentially affected by this Incident. Of those, 49 were residents of Maine. Notification letters to these individuals were mailed on April 14, 2025, by first class mail. A sample copy of the notification letter is included with this letter under **Exhibit A**.

3. Steps taken in response to the Incident.

Data privacy and security are among MedEx's highest priorities, and there are extensive measures in place to protect information in MedEx's care. Since the discovery of the Incident, MedEx moved quickly to investigate, respond, and confirm the security of their systems. Specifically, MedEx engaged a specialized third-party cybersecurity firm, changed administrative credentials, notified law enforcement, and continues to enhance its network security to prevent a similar incident from occurring in the future. Additionally, MedEx took the following steps, including, but not limited to: disconnecting all access to the network; implementing an organization-wide credential reset of all users; restructured and enhanced security systems, and upgrading their data management software. Lastly, MedEx informed our law firm and began identifying the potentially affected individuals in preparation for notice.

Although MedEx is not aware of any actual or attempted misuse of the affected personal information, MedEx offered 12 months of complimentary credit monitoring and identity theft restoration services through Haystack to individuals who has sensitive personal information impacted to help protect their identity. Additionally, MedEx 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

MedEx 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 312.821.6141 or joseph.fusz@wilsonelser.com.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Joseph M. Fusz

EXHIBIT A

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Via First-Class Mail

[redacted]

April 14, 2025

RE: Notice of Data Breach

Dear [redacted]

Medical Express Ambulance Inc. D/B/A MedEx Ambulance ("MedEx") is writing to inform you of a recent data security incident that may have resulted in an unauthorized access to your sensitive personal information. 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. Please be assured MedEx takes the protection and proper use of your personal information very seriously.

What Happened?

On March 18, 2024, MedEx experienced a network disruption that impacted the functionality and access of certain systems. Upon discovery of this incident, MedEx 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 forensic investigation determined that that personal information may have been acquired by the threat actor.

Based on these findings, MedEx decided to proceed with an analysis of the compromised data for any potential sensitive personal information ("PII") or protected health information ("PHI"). MedEx engaged a third-party vendor to review the data that was compromised. The data mining process took some time given the complexities of the types and the volume of the data analyzed, requiring multiple phases of automated and manual review. On March 3, 2025, MedEx engaged a third-party notice vendor to assist with the mailings, call center, and provide identity theft protection services. Thereafter, MedEx worked to verify the patient information and addresses for mailing. On March 19, 2025, MedEx finalized the list of individuals to notify.

What Information was Involved?

Although MedEx 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. The information impacted varied by individual. Based on the investigation, the following information related to you may have been subject to unauthorized access: Name, Date of Birth, Social Security Number, Driver's License or State ID and Health Insurance Information.

What We Are Doing:

Data privacy and security are among MedEx's highest priorities, and there are extensive measures in place to protect information in MedEx's care. Since the discovery of the Incident, MedEx moved quickly to investigate, respond, and confirm the security of our systems. Specifically, MedEx engaged a specialized third-party cybersecurity firm, changed administrative credentials, notified law enforcement, and continues to enhance its network security to prevent a similar incident from occurring in the future. Additionally, MedEx took the following steps, including, but not limited to: disconnecting all access to the network; implementing an organization-wide credential reset of all users; restructured and enhanced security systems, and upgrading our data management software.

In light of the incident, we are also providing you with 12 months of complimentary credit monitoring and identity theft restoration services through HaystackID. 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 *Additional Resources 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 July 10, 2025.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to www.privacysolutions.com 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 855-659-0097 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

MedEx 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,

Medical Express Ambulance Services

ADDITIONAL RESOURCES TO HELP PROTECT YOUR INFORMATION

Monitor Your Accounts

We recommend that you remain vigilant for incidents of fraud or identity theft by regularly reviewing your credit reports and financial accounts for any suspicious activity. You should contact the reporting agency using the phone number on the credit report if you find any inaccuracies with your information or if you do not recognize any of the account activity.

You may obtain a free copy of your credit report by visiting www.annualcreditreport.com, calling toll-free at 1-877-322-8228, or by mailing a completed Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report for a fee by contacting one or more of the three national credit reporting agencies.

You have rights under the federal Fair Credit Reporting Act (FCRA). The FCRA governs the collection and use of information about you that is reported by consumer reporting agencies. You can obtain additional information about your rights under the FCRA by visiting https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act.

Credit Freeze

You have the right to add, temporarily lift and remove a credit freeze, also known as a security freeze, on your credit report at no cost. A credit freeze prevents all third parties, such as credit lenders or other companies, whose use is not exempt under law, from accessing your credit file without your consent. If you have a freeze, you must remove or temporarily lift it to apply for credit. Spouses can request freezes for each other as long as they pass authentication. You can also request a freeze for someone if you have a valid Power of Attorney. If you are a parent/guardian/representative you can request a freeze for a minor 15 and younger. To add a security freeze on your credit report you must make a separate request to each of the three national consumer reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The following information must be included when requesting a security freeze: (i) full name, with middle initial and any suffixes; (ii) Social Security number; (iii) date of birth (month, day, and year); (iv) current address and any previous addresses for the past five (5) years; (v) proof of current address (such as a copy of a government-issued identification card, a recent utility or telephone bill, or bank or insurance statement); and (vi) other personal information as required by the applicable credit reporting agency.

Fraud Alert

You have the right to add, extend, or remove a fraud alert on your credit file at no cost. A fraud alert is a statement that is added to your credit file that will notify potential credit grantors that you may be or have been a victim of identity theft. Before they extend credit, they should use reasonable procedures to verify your identity. Please note that, unlike a credit freeze, a fraud alert only notifies lenders to verify your identity before extending new credit, but it does not block access to your credit report. Fraud alerts are free to add and are valid for one year. Victims of identity theft can obtain an extended fraud alert for seven years. You can add a fraud alert by sending your request to any one of the three national reporting agencies by phone, online, or by mail by following the instructions found at their websites (see "Contact Information" below). The agency you contact will then contact the other credit agencies.

Federal Trade Commission

For more information about credit freezes and fraud alerts and other steps you can take to protect yourself against identity theft, you can contact the Federal Trade Commission (FTC) at 600 Pennsylvania Avenue NW, Washington, DC 20580, 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.

You should also report instances of known or suspected identity theft to local law enforcement and the Attorney General's office in your home state and you have the right to file a police report and obtain a copy of your police report.

Contact Information

Below is the contact information for the three national credit reporting agencies (Experian, Equifax, and TransUnion) if you would like to add a fraud alert or credit freeze to your credit report.

Credit Reporting Agency	Access Your Credit Report	Add a Fraud Alert	Add a Security Freeze
Experian	P.O. Box 2002 Allen, TX 75013-9701 1-866-200-6020 www.experian.com	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 https://www.experian.com/fraud/center.html	P.O. Box 9554 Allen, TX 75013-9554 1-888-397-3742 www.experian.com/freeze/center.html
Equifax	P.O. Box 740241 Atlanta, GA 30374-0241 1-866-349-5191 www.equifax.com	P.O. Box 105069 Atlanta, GA 30348-5069 1-800-525-6285 www.equifax.com/personal/credit-report-services/credit-fraud-alerts	P.O. Box 105788 Atlanta, GA 30348-5788 1-888-298-0045 www.equifax.com/personal/credit--report-services
TransUnion	P.O. Box 1000 Chester, PA 19016-1000 1-800-888-4213 www.transunion.com	P.O. Box 2000 Chester, PA 19016 1-800-680-7289 www.transunion.com/fraud-alerts	P.O. Box 160 Woodlyn, PA 19094 1-800-916-8800 www.transunion.com/credit-freeze

Iowa and Oregon residents are advised to report suspected incidents of identity theft to local law enforcement, to their respective Attorney General, and the FTC.

Massachusetts residents are advised of their right to obtain a police report in connection with this incident.

District of Columbia residents are advised of their right to obtain a security freeze free of charge and can obtain information about steps to take to avoid identity theft by contacting the FTC (contact information provided above) and the Office of the Attorney General for the District of Columbia, Office of Consumer Protection, at 400 6th St. NW, Washington, D.C. 20001, by calling the Consumer Protection Hotline at (202) 442-9828, by visiting https://oag.dc.gov, or emailing at consumer.protection@dc.gov.

Maryland residents can obtain information about steps they can take to avoid identity theft by contacting the FTC (contact information provided above) or the Maryland Office of the Attorney General, Consumer Protection Division Office at 44 North Potomac Street, Suite 104, Hagerstown, MD 21740, by phone at 1-888-743-0023 or 410-528-8662, or by visiting http://www.marylandattorneygeneral.gov/Pages/contactus.aspx.

New York residents are advised that in response to this incident they can place a fraud alert or security freeze on their credit reports and may report any incidents of suspected identity theft to law enforcement, the FTC, the New York Attorney General, or local law enforcement. Additional information is available at the website of the New York Department of State Division of Consumer Protection at https://dos.nysits.acsitefactory.com/consumerprotection; by visiting the New York Attorney General at https://ag/ny.gov or by phone at 1-800-771-7755; or by contacting the FTC at www.ftc.gov/bcp/edu/microsites/idtheft/ or https://www.identitytheft.gov/#/.

North Carolina residents are advised to remain vigilant by reviewing account statements and monitoring free credit reports and may obtain information about preventing identity theft by contacting the FTC (contact information provided above) or the North Carolina Office of the Attorney General, Consumer Protection Division at 9001 Mail Service Center, Raleigh, NC 27699-9001, or visiting www.ncdoj.gov, or by phone at 1-877-5-NO-SCAM (1-877-566-7226) or (919) 716-6000.

Rhode Island residents are advised that they may file or obtain a police report in connection with this incident and place a security freeze on their credit file and that fees may be required to be paid to the consumer reporting agencies.