



Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

Dear <<Full Name>>:

Acadian Ambulance Service, Inc. (“Acadian”) is writing to inform you of a recent event that may impact the privacy of some of your information. Although at this time there is no indication that your information has been used to commit identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and steps you may take to help protect your information, should you feel it necessary to do so.

What Happened? On or around June 21, 2024, we became aware of suspicious activity relating to certain systems within our network. We immediately took steps to secure our systems and launched an investigation with the assistance of third-party computer specialists to confirm the full nature and scope of the activity and to restore functionality to the affected systems. The investigation determined there was unauthorized access to Acadian’s network between June 19, 2024, and June 21, 2024, and that certain files and folders were or may have been taken without authorization during that time. Upon becoming aware of this information, Acadian began a diligent and comprehensive review process to identify sensitive information that was contained within the impacted files, and to identify the individuals whose information may have been impacted. Acadian then worked to identify appropriate contact information for the impacted individuals. That process was recently completed, and we are notifying you because the investigation determined certain information related to you was contained within the impacted files.

What Information Was Involved? The investigation determined the following types of information related to you were present in the impacted systems and were or may have been taken without authorization: name, address <<data elements>> and medical information collected during the patient intake process, which could include diagnosis, disability information, medications, and treatment information.

What We Are Doing. The confidentiality, privacy, and security of information within our care are among Acadian’s highest priorities. Upon learning of the event, we promptly commenced an investigation and response that included confirming the security of our systems, reviewing the contents of relevant data for sensitive information, and investigating to determine the information that may be impacted. We also reported this event to federal law enforcement and government regulators. As part of our ongoing commitment to the privacy of information in their care, we are reviewing its policies, procedures and processes to reduce the likelihood of a similar future event.

Although we have no evidence of identity theft or fraud occurring as the result of this incident, as an added precaution, we are also offering you <<12/24>> months of credit monitoring and identity restoration services at no cost to you through CyEx. Enrollment instructions are enclosed with this letter.

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 credit reports for suspicious activity and to detect errors. Please review the enclosed *Steps You Can Take to Help Protect Personal Information* for useful information on what you can do to better protect

against possible misuse of information. You may also enroll in the complimentary credit monitoring services we have provided for you.

For More Information. If you have additional questions, you may call our assistance line at 855-278-0575 (toll free), Monday through Friday, 9:00 AM to 9:00 PM Eastern Time, excluding U.S. holidays. You may also write to Acadian at P.O. Box 93088, Lafayette, LA 70509.

Sincerely,

Acadian Ambulance Services, Inc.

Steps You Can Take to Help Protect Personal Information

Enroll in Credit Monitoring Services



Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>
Service Term: <<12/24>> months*

Identity Defense Complete

Key Features

- 1-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/aasi

1. **Enter your unique Activation Code <<Activation Code>>**
Enter your Activation Code and click 'Redeem Code'.
2. **Create Your Account**
Enter your email address, create your password, and click 'Create Account'.
3. **Register**
Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.
4. **Complete Activation**
Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at 1.866.622.9303.

*Service Term begins on the date of enrollment, provided that the enrollment takes place during the approved enrollment period.

Monitor 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 your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your 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 one-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 you are a victim of identity

theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one 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 your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report 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 security freeze, you will need to provide 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, military identification, etc.); 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:

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 state attorney general. This notice has not been delayed by law enforcement.

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>.