



L. Judson Welle
Partner
JWelle@goodwinlaw.com

Goodwin Procter LLP
The New York Times Building
620 Eighth Avenue
New York, NY 10018

goodwinlaw.com
+1 212 813 8800

December 27, 2023

VIA EMAIL [\[IDTHEFT@OAG.STATE.MD.US\]](mailto:IDTHEFT@OAG.STATE.MD.US)

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: Notice Pursuant to *MD Commercial Code* § 14–3501(e)

Dear Attorney General Brown:

Pursuant to *Maryland Commercial Code* section 14–3501(e), we write on behalf of Fallon Ambulance Services (“Fallon” or “Company”), which was a subsidiary of Transformative Healthcare until it ceased operations in 2022, to notify you of a data security matter, which we believe may have affected approximately **1,578** Maryland residents. Fallon was a medical transportation company that, in part, responded to patient emergencies in the greater Boston area and provided administrative services for affiliated medical transportation companies. Fallon ceased operations in December 2022 but, to comply with legal obligations, has maintained an archived copy of data previously stored on its computer systems.

On or around April 21, 2023, after Fallon had ceased operations, it detected suspicious activity within its data storage archive. Fallon promptly took steps to secure the archive and initiated a comprehensive investigation into the matter with the assistance of third-party specialists. After an extensive review of the event, Fallon identified that the activity appears to have occurred as early as February 17, 2023 through April 22, 2023 and that files were obtained by an unauthorized party that may have contained personal information. Fallon then conducted a comprehensive evaluation of the potentially impacted files to determine the nature of any personal information contained therein and to identify the current mailing address for potentially impacted individuals. This process was completed on or around December 27, 2023. Based on this review, Transformative determined that the impacted files may have included personal information of **1,578** Maryland residents.

The types of information that may have been impacted will depend on the information provided to Fallon about the individual, but may include: name, address, Social Security number, medical information, including COVID-19 testing or vaccination information, and information provided to Fallon in connection with employment or application for employment. Notification of this matter was mailed to the impacted residents on or around December 27, 2023.

While Fallon is no longer operational, it nonetheless takes the protection of information seriously and has taken steps to secure data that may be stored in its archives for compliance with its legal obligations. While Fallon currently has no evidence of identity theft or fraud related to consumer information as a result of this matter, the Company is also offering two years of identity protection services, at no cost, to



Office of the Attorney General
Page 2

affected individuals through IDX. Fallon also consulted with federal law enforcement in support of its investigation and response to this matter.

Should you have any questions about this matter, please do not hesitate to contact me directly, by phone or email. Thank you for your attention to this matter.

Sincerely,

L. Judson Welle



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://response.idx.us/Fallon>

December 27, 2023

RE: NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

We are contacting you to provide information regarding a security incident at Fallon Ambulance Service ("Fallon") that may have impacted some of your information and to inform you about steps you may take to help protect your information. Fallon was a medical transportation company that, in part, responded to patient emergencies in the greater Boston area and provided administrative services for affiliated medical transportation companies. Fallon ceased operations in December 2022 but, to comply with legal obligations, has maintained an archived copy of data previously stored on its computer systems.

What Happened

On or around April 21, 2023, after Fallon had ceased operations, we detected suspicious activity within our data storage archive. We promptly took steps to secure the archive and initiated a comprehensive investigation into the matter with the assistance of third-party specialists. After an extensive review of the event, we identified that the activity appears to have occurred as early as February 17, 2023 through April 22, 2023 and that files were obtained by an unauthorized party that may have contained personal information. We then conducted a comprehensive evaluation of the potentially impacted files to determine the nature of any personal information contained therein and to identify the current mailing address for potentially impacted individuals. This process was completed on or around December 27, 2023. Based on our review, we determined that the impacted files may have included certain of your personal information.

While we currently have no evidence of identity theft or fraud related to your information as a result of this matter, we are notifying you to provide you with information and steps you can take to help protect your information.

What Information Was Involved

The types of information that may have been impacted will depend on the information provided to Fallon but may include: <<Variable Text Data Elements>>. *Again, at this time, we have no evidence of identity theft or fraud related to your personal information as a result of this incident.*

What We Are Doing

We take the protection of your information very seriously, and we sincerely regret that this incident occurred. While Fallon is no longer operational, we have taken steps to secure data that may be stored in our archives for compliance with our legal obligations. Additionally, to help further protect your information, we are providing you with **free**

identity protection services for two years, as described in detail in this letter. We also consulted with federal law enforcement in support of our investigation and response to this matter.

What You Can Do

There are steps you can take to help protect your information, including enrolling in the identity protection service we are offering to you for free. As a best practice, we encourage you to remain vigilant for suspicious activity and to regularly review your financial statements and credit reports.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-888-317-9491, going to <https://response.idx.us/Fallon>, or scanning the QR image and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is March 27, 2024.

For More Information

In addition to the information provided in this letter, we have also enclosed an attachment with additional information and resources. Please note, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please retain this letter for your enrollment.

If you have any additional questions, you can call 1-888-317-9491 or go to <https://response.idx.us/Fallon> for assistance or for any additional questions you may have.

Sincerely,

A handwritten signature in black ink, appearing to read 'Tom', is positioned above the printed name of the sender.

Thomas McEntee, CEO
Transformative

(Enclosure)

ADDITIONAL RESOURCES

The following provides additional information and actions that you can consider taking to help protect your information. You may also contact the U.S. Federal Trade Commission ("FTC"), the credit reporting agencies, or your state's regulatory authority to obtain additional information about avoiding identity theft, including information about fraud alerts and security freezes, as further detailed below. Contact Information for the Federal Trade Commission and credit reporting agencies is set forth below:

The Federal Trade Commission

600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

Credit Reporting Agencies

Equifax

PO Box 740241
Atlanta, GA 30374
1-800-525-6285
www.equifax.com

Experian

PO Box 4500
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

PO Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com

Order Your Free Annual Credit Report. You can order your free annual credit report online at www.annualcreditreport.com, by phone (toll free) at 877-322-8228, or by mail by submitting a completed Annual Credit Report Request Form to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can download a copy of the request form on the FTC website: www.ftc.gov. You can also visit the Consumer Financial Protection Bureau's website for more information on how you can obtain your credit report for free: www.consumerfinance.gov. Once you receive your credit reports, review them carefully for any discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting agency.

Review Your Accounts and Report Unauthorized Activity. We recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the FTC. Carefully review your credit reports and bank, credit card, and other account statements. Be proactive and create alerts on credit cards and bank accounts to notify you of activity. If you discover unauthorized or suspicious activity on your credit report or by any other means, file an identity theft report with your local police and contact a credit reporting company. You may also consider filing or obtaining a police report.

Consider Placing a Fraud Alert on Your Credit File. To protect yourself from potential identity theft, you may consider placing a fraud alert on your credit file. A fraud alert is intended to make it more difficult for someone to open a new credit account in your name. A fraud alert indicates to an entity requesting your credit file that you suspect you are a victim of fraud. When you or someone else attempts to open a credit account in your name, increase the credit limit on an existing account, or obtain a new card on an existing account, the alert notifies the entity to take steps to verify your identity. You may contact one of the credit reporting agencies listed above for assistance.

Consider Placing a Security Freeze on Your Credit File. You also may consider implementing a security freeze (also called a "credit freeze"). Placing a freeze on your credit report restricts access to your credit report and will prevent lenders and others from accessing your credit report entirely. This means you (or others) will not be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. With a security freeze in place, you may be required to take special steps when you wish to apply for any type of credit. You may contact one of the credit reporting agencies listed above for assistance.

Remain Vigilant and Lookout for Phishing Schemes. We also encourage you to remain vigilant in managing and handling your personal information and be on the lookout for suspicious emails, such as phishing schemes. Phishing

schemes are attempts by criminals to steal personal information, including credit card numbers and social security numbers, over email. These attempts are often made by manipulating an email to make it look as if it came from a legitimate source, but which are actually sent by a fraudulent impersonator. Pay particular attention to anyone asking you to click on a link or attachment, especially if the email requests sensitive information, and pay close attention to the email address (e.g., look for misspellings). It is also important that you check the recipient's email address when replying to emails to ensure it is legitimate. Also consider taking steps such as carrying only essential documents with you, being aware of how and with whom you are sharing your personal information, and shredding receipts, statements, and other sensitive information once you no longer need them.

For District of Columbia Residents: You may also obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia:

Office of the Attorney General for the District of Columbia

Office of Consumer Protection

400 6th Street NW

Washington, D.C. 20001

(202) 442-9828

<https://oag.dc.gov/>

For Maryland Residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General:

Maryland Office of the Attorney General

Consumer Protection Division

200 St. Paul Place

Baltimore, MD 21202

1-888-743-0023

<http://www.marylandattorneygeneral.gov>

For New York Residents: You may also obtain information about preventing and avoiding identity theft from the New York Attorney General's Office or New York's Office of Information Technology Services:

New York Attorney General's Office

Office of the Attorney General

The Capitol

Albany, NY 12224-0341

1-800-771-7755

<https://ag.ny.gov/>

New York Office of Information Technology Services

Empire State Plaza

P.O. Box 2062

Albany, NY 12220-0062

844-891-1786

<https://its.ny.gov/>

For North Carolina Residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office:

North Carolina Attorney General's Office

Consumer Protection Division

9001 Mail Service Center

Raleigh, NC 27699-9001

1-877-5-NO-SCAM

www.ncdoj.gov

For Rhode Island Residents: You have the right to obtain a police report. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General:

Rhode Island Office of the Attorney General

Consumer Protection Unit

150 South Main Street

Providence, RI 02903

1-401-274-4400

<https://riag.ri.gov/>