<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

On behalf of MedStar Mobile Healthcare, the emergency and non-emergency ambulance service provider for 15 cities in Tarrant County, Texas, we are writing to inform you that we recently suffered a cyberattack affecting portions of protected health information for individuals we have served, which may have included your information. On October 20, 2022, we experienced issues with our network systems. We promptly investigated and determined that a third party had accessed our network. MedStar is providing this notice to give you more information on what happened and what we are doing in response.

WHAT HAPPENED

An unauthorized third party gained access to a restricted location in MedStar's computer network that contained a number of files, including those with personal health information. We have not been able to confirm that those files were actually accessed by the third party, and therefore cannot say that any of your information in those files was accessed. Nevertheless, in an abundance of caution and out of respect for those individuals we have served, we are providing this notice to alert you to the potential that your information was impacted by this incident.

WHAT INFORMATION WAS INVOLVED

These files contained information for individuals who received treatment and care from MedStar. For the large majority of individuals, only non-financial billing information was involved. For a portion of individuals, however, the impacted information may include full name, date of birth, contact information, and information related to medical care provided.

WHAT WE ARE DOING

We have security measures in place that allow us to take prompt action against attempted intrusions into our network. Those measures were implemented here and reduced the scope of the third party's activity. We also hired third-party experts to help us investigate the extent of the incident, and we are further securing our systems to protect the information we maintain. And we continue to investigate the full scope of the incident.

WHAT YOU CAN DO

If you have questions about this matter, please call us at the phone number below. While the information involved generally poses a lower risk of identity theft or fraud, we nonetheless encourage you to remain vigilant for such activity. Enclosed with this letter you will find additional steps you can take to protect yourself.

FOR MORE INFORMATION

Our patients and their information are important to us. Should you have any questions, you can contact us at xxx-xxx-xxxx, Monday through Friday 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays, and one of our representatives will be happy to assist you. Thank you for your understanding and patience.

Sincerely,

Kenneth J. Simpson, JD, NRP
Chief Executive Officer
MedStar Mobile Healthcare

ELN-16536

ADDITIONAL STEPS YOU CAN TAKE

Remain vigilant – Review your account statements and free credit reports.

- You should confirm that your credit card company has the correct address on file for you and that all charges on the account are legitimate. If you discover errors or suspicious activity, you should immediately contact the credit card company and inform them that you have received this letter.
- You should obtain and review a free copy of your credit report by visiting www.annualcreditreport.com or calling 1-877-322-8228. If the report is incorrect, you should contact the appropriate consumer reporting agency—Equifax, Experian, or TransUnion.

Consider placing a fraud alert or security freeze on your credit file – Consumer reporting agencies have tools you can use to protect your credit, including fraud alerts and security freezes.

- A fraud alert is a cautionary flag you can place on your credit file to notify companies extending you credit that they should take special precautions to verify your identity. You can contact any of the three consumer reporting agencies to place fraud alerts with each agency.
- A security freeze is a more dramatic step that will prevent others from accessing your credit report, which will prevent them from extending you credit. You must contact each consumer reporting agency separately to order a security freeze, and they may require you to provide them with your full name, Social Security number, date of birth, and current and previous addresses. You can obtain more information about security freezes by contacting the consumer reporting agencies or the Federal Trade Commission.

Report suspicious activity – If you believe you are the victim of identity theft, consider notifying your Attorney General, local law enforcement, or the Federal Trade Commission. You can also file a police report concerning the suspicious activity and request a copy of that report.

Contact relevant authorities – You may contact the below resources to (1) get more information on fraud alerts or security freezes and (2) learn more about protecting yourself from fraud or identity theft.

Federal Trade Commission	**Equifax**	**Experian**	**TransUnion**
600 Pennsylvania Ave. NW	P.O. Box 740241	P.O. Box 9701	P.O. Box 2000
Washington, DC 20580	Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
(202) 326-2222	(800) 685-1111	(888) 397-3742	(888) 909-8872
www.ftc.gov	www.equifax.com	www.experian.com	www.transunion.com