Guidehouse

July 29, 2021

Office of Consumer Protection
555 Fuller Avenue
Helena, MT 59601
Fax: (406) 442-2174

To Whom It May Concern:

I write on behalf of Guidehouse, a global provider of professional services, to inform you about an incident in which personal information relating to Montana residents was accessed by an unauthorized third party. Guidehouse, a provider of professional services, provides business consulting services to Lehigh Valley Health Network.

On March 23, 2021, we received reports that certain of our data might have been impacted as part of a cyber-attack campaign that targeted the Accellion File Transfer Appliance ("FTA") product that was used by Guidehouse and many other companies. (For information that Accellion has provided publicly about the compromise of its product, see https://www.accellion.com/company/security-updates/accellion-responds-to-recent-fta-security-incident/ and https://www.accellion.com/company/security-updates/mandiant-issues-final-report-regarding-accellion-fta-attack/).

Upon learning of the incident, we immediately launched an investigation, and have since ceased using the third-party service that had been compromised. We have cooperated with federal law enforcement and engaged leading cyber security experts in connection with investigating and responding to the incident. Based on our investigation, we determined that the threat actor entered the Accellion FTA system and exploited a vulnerability in it on January 20, 2021. Due to the nature of the incident, it has taken time to accurately determine what data was impacted. Through the investigation, we have determined that the third party accessed the medical record number, account number(s), date(s) of service, diagnosis and procedure name, insurance information and provider name of individual patients of our client Lehigh Valley Health Network. After determining Lehigh Valley Health Network information was impacted, we notified Lehigh Valley Health Network on June 4, 2021. We are not aware of any misuse of the information.

We will notify one Montana resident of this incident, beginning on July 29, 2021. While we do not believe the information involved in this incident will cause credit or identity theft issues, we will provide this individual with an offer for complimentary two year credit monitoring service provided by Experian. An individual can enroll in Experian's IdentityWorks credit monitoring product either online at https://www.experianidworks.com/credit or by calling (855) 797-1889.

Attached is a sample of the letter that we are providing to Montana residents.

Guidehouse

Please do not hesitate to contact me at (202) 973-4572 if you have any questions.

Sincerely,

Shamir Patel
Deputy General Counsel

Guidehouse

Return Mail Processing
PO Box 999
Suwanee, GA 30024

148 1 35936 **********AUTO**5-DIGIT 19540
SAMPLE A. SAMPLE - L01
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

July 29, 2021

Notice of Data Breach

I am writing on behalf of Guidehouse, a global provider of professional services, to inform you about an incident that involved personal information about you. We regret that this incident occurred and take the security of personal information seriously.

WHAT HAPPENED. We learned in late March 2021 that we had been the victim of a cyber-attack. The attack occurred in late January 2021, and involved the compromise of a third-party service used for secure file transfer for many clients including Lehigh Valley Health Network. Guidehouse provides business consulting services to Lehigh Valley Health Network.

WHAT INFORMATION WAS INVOLVED. We have determined that the personal information involved in this incident may have included your medical record number, account number(s), date(s) of service, diagnosis and procedure name, insurance information and provider name.

WHAT WE ARE DOING. Upon learning of the incident, we immediately launched an investigation, and have since ceased using the third-party service that had been compromised. We have cooperated with federal law enforcement and engaged leading cyber security experts in connection with investigating and responding to the incident. Based on the nature of the incident, it has taken time to accurately determine what data was impacted. After determining Lehigh Valley Health Network information was impacted, we notified Lehigh Valley Health Network on June 4, 2021.

WHAT YOU CAN DO. We are not aware of any misuse of your information. Consistent with certain laws, we are providing you with the following information about steps that a consumer can take to protect against potential misuse of personal information.

While we do not believe that the information involved in this incident will cause credit or identity theft issues, as a precaution, we have arranged for you, at your option, to enroll in a complimentary, two-year credit monitoring service. We have engaged Experian to provide you with its IdentityWorks credit monitoring product. This product provides you with superior identity detection and resolution of identity theft. You have until October 31, 2021 to activate the free credit monitoring service by using the following activation code: **ABCDEFGHI.** This code is unique for your use and should not be shared. To enroll, please go to https://www.experianidworks.com/credit or call (855) 797-1889.

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (855) 797-1889 by October 31, 2021. Be prepared to provide engagement number **B016325** as proof of eligibility for the identity restoration services by Experian.

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your state Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's Web site, at www. ftc.gov/idtheft, or call the FTC, at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.Equifax.com/personal/ credit-report-services	www.Experian.com/help	Chester, PA 19022 www.TransUnion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the phone numbers listed above to place a security freeze to restrict access to your credit report.

You will need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.

Please know that we regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us at (855) 797-1889 if you have any questions or concerns.

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
441 4th Street, NW
Suite 1100 South
Washington, DC 20001
(202) 727-3400
https://oag.dc.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
http://www.ftc.gov/idtheft/

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.oag.state.md.us

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

New York Attorney General
Consumer Frauds &
Protection Bureau
120 Broadway, 3rd Floor
New York, NY 10271
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, New York 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.gov/idtheft

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
http://www.ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: This incident impacted two Rhode Island residents. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
http://www.riag.ri.gov/