LEWIS BRISBOIS BISGAARD & SMITH LLP

Elizabeth R. Dill
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Elizabeth.Dill@lewisbrisbois.com
Direct: 215.977.4080

October 25, 2020

VIA WEBSITE SUBMISSION
Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: Notification of Data Security Incident

Dear Attorney General Frey:

We represent Centerstone of Tennessee, Inc. ("Centerstone") in connection with a data security incident which is described in greater detail below. Centerstone takes the protection of all sensitive information within its possession very seriously and is taking steps to prevent similar incidents from occurring in the future.

1. **Nature of the security incident.**

Centerstone learned of unusual activity involving an employee's email account. Upon discovering this activity, Centerstone immediately launched an investigation. In the course of this investigation, Centerstone engaged an independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that two Centerstone of Tennessee employee email accounts had been accessed without authorization between December 12 and December 16, 2019. On August 25, 2020, Centerstone learned that personal information and protected health information belonging to certain current/former patients and staff was contained within the impacted email accounts. Centerstone then took steps to identify current mailing addresses in order to notify the potentially affected individuals. On October 19, 2020, Centerstone became aware of 1 Maine resident within the potentially affected population.

The information involved in this incident included the Maine resident's name and Social Security number.

Centerstone is not aware of any misuse of the information involved in the incident. Additionally, this unauthorized access was limited to information transmitted via email and did not affect any other Centerstone information systems.

2. Number of Maine residents affected.

Centerstone issued notification letters to the one (1) Maine resident regarding this data security incident via first-class U.S. mail on October 22, 2020. A sample copy of the notification letter that was sent to the affected individuals is attached hereto.

3. Steps taken relating to the incident.

Centerstone has taken steps in response to this incident to prevent similar incidents from occurring in the future. Those steps have included conducting cybersecurity assessments of its systems, training users to increase awareness of phishing and other cybersecurity risks, and updating additional technical safeguards and policies to further increase the security of its email environment. Centerstone is also offering credit monitoring and identity protection services at no cost to affected individuals through IDX. Centerstone reported the incident to the Department of Health and Human Services Office for Civil Rights on October 23, 2020.

4. Contact information.

Centerstone remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at (215) 977-4080 or via email at Elizabeth.Dill@lewisbrisbois.com.

Regards,

Elizabeth R. Dill of
LEWIS BRISBOIS BISGAARD & SMITH LLP

ERD:ALW

Attachment: Consumer Notification Letter Template

To Enroll, Please Call:
1-833-752-0854
Or Visit:
https://response.idx.us/centerstone
Enrollment Code: <<XXXXXXXX>>

October 22, 2020

Subject: Notice of Data Security Incident

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

I am writing to inform you of a data security incident that may have affected your personal information. At Centerstone of Tennessee, Inc. ("Centerstone"), we take the privacy and security of your personal information very seriously. We are contacting you to notify you that this incident occurred and inform you about steps you can take to ensure your information is protected, including enrolling in the complimentary identity protection services we are making available to you.

What Happened? Centerstone learned of unusual activity involving an employee's email account. Upon discovering this activity, we immediately launched an investigation. In the course of this investigation, we engaged an independent computer forensics firm to determine what happened and whether personal information had been accessed or acquired without authorization. The forensic investigation concluded that two employee email accounts had been accessed without authorization between December 12 and December 16, 2019. On August 25, 2020, we learned that some of your information was contained within one of these email accounts. As soon as we discovered that the incident impacted personal information, we immediately conducted a diligent search to identify current mailing addresses so that we could notify potentially impacted individuals.

Please note that this unauthorized access was limited to information transmitted via email and did not affect any other Centerstone information systems. We are not aware of the misuse of any personal information that may have been affected by this incident.

What Information Was Involved? The affected information pertaining to you may have included the following: <<Information Affected>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. We have also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future. In addition, we are providing you with information about steps that you can take to help protect your personal information and, out of an abundance of caution, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised. Please note that the deadline to enroll in these services is January 22, 2021.

What Can You Do? We recommend that you review the guidance included with this letter about how to protect your information. You can also contact our dedicated call center with any questions and to enroll in the free services by calling 1-833-752-0854 or by going to https://response.idx.us/centerstone and using the Enrollment Code provided above. Call center representatives are available to assist you Monday through Friday from 8 am – 8 pm Central Standard Time.

For More Information: Further information about how to help protect your personal information appears on the following page. If you have questions or need assistance, please call 1-833-752-0854, Monday through Friday from 8 am – 8 pm Central Standard Time.

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

David C. Guth, Jr.
Chief Executive Officer
Centerstone

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You should also promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (the "FTC").

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com/, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can also contact one of the following three national credit reporting agencies:

Equifax	**Experian**	**TransUnion**	**Free Annual Report**
P.O. Box 105851	P.O. Box 9532	P.O. Box 1000	P.O. Box 105281
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-800-525-6285	1-888-397-3742	1-877-322-8228	1-877-322-8228
www.equifax.com	www.experian.com	www.transunion.com	www.annualcreditreport.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. There is no charge to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state. Contact information for the FTC is: **Federal Trade Commission**, 600 Pennsylvania Ave, NW, Washington, DC 20580, www.consumer.ftc.gov or www.ftc.gov/idtheft, 1-877-438-4338.

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include knowing what is in your file; disputing incomplete or inaccurate information; and requiring consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

Personal Information of a Minor: You can request that each of the three national credit reporting agencies perform a manual search for a minor's Social Security number to determine if there is an associated credit report. Copies of identifying information for the minor and parent/guardian may be required, including birth or adoption certificate, Social Security card and government issued identification card. If a credit report exists, you should request a copy of the report and immediately report any fraudulent accounts to the credit reporting agency. You can also report any misuse of a minor's information to the FTC at https://www.identitytheft.gov/. For more information about Child Identity Theft and instructions for requesting a manual Social Security number search, visit the FTC website: https://www.consumer.ftc.gov/articles/0040-child-identity-theft. Contact information for the three national credit reporting agencies may be found below