



Aubrey L. Weaver
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Aubrey.Weaver@lewisbrisbois.com
Direct: 215.253.7506

September 14, 2022

VIA ELECTRONIC MAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois represents Centerstone of Tennessee, Inc. ("Centerstone"), a nonprofit health system providing mental health and substance use disorder treatments, in connection with a recent data security incident described in greater detail below. This letter is being sent because the personal information of two (2) Maryland residents may have been involved in this incident.

1. Nature of the Security Incident

On February 14, 2022, Centerstone detected unusual activity within its email environment. Upon discovering this activity, Centerstone took immediate steps to secure its email environment and launched a thorough investigation to determine the scope of the issue. The investigation determined that one employee email account may have been accessed without authorization on January 8, 2022.

As a result, Centerstone undertook a comprehensive review of the full contents of the email account to identify what information may have been involved in the incident. Centerstone's review concluded on July 12, 2022, at which time it learned that the email accounts contained certain personal and protected health information. Since that time, Centerstone has been working diligently to identify current contact information needed to notify all individuals potentially affected by this incident.

2. Type of Information and Number of Maryland Residents Affected

Centerstone notified the two (2) potentially affected Maryland residents of this incident via first class U.S. mail beginning on September 12, 2022. The potentially affected data elements include the individuals' names, Social Security numbers, health information, and/or health insurance information. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident

As soon as Centerstone discovered this incident, it took steps to secure its systems and launched an investigation to determine what happened and whether personal or protected health information had been accessed or acquired without authorization. Centerstone has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future. These include resetting credentials to all potentially affected accounts, revising Centerstone's mobile device and email syncing policies, and further increasing its password complexity requirements.

Centerstone has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, Centerstone is offering twelve (12) months of complimentary credit and identity monitoring services to the potentially affected individuals whose Social Security numbers may have been involved in the incident. Centerstone has also reported the incident to the Department of Health and Human Services Office for Civil Rights.

4. Contact Information

Centerstone remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at (215) 253-7506 or by e-mail at Aubrey.Weaver@lewisbrisbois.com.

Sincerely,

Aubrey L Weaver of
LEWIS BRISBOIS BISGAARD & SMITH LLP

ALW:AME

Encl.: Consumer Notification Letter Template



CENTERSTONE

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

To Enroll, Please Call:

1-833-764-0234

Or Visit:

<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

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

September 12, 2022

Subject: Notice of Data <<Variable 3>>

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a data security incident that may have affected your information. At Centerstone of Tennessee, Inc. ("Centerstone"), we take the privacy and security of your 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? In February 2022, Centerstone learned of unusual activity involving an employee's email account. Upon discovering this activity, we immediately launched an investigation, which concluded that an employee email account may have been accessed without authorization on January 8, 2022. As a result, we undertook a comprehensive review of the contents of the email accounts to identify whether any individual information was contained therein. Our review concluded on July 12, 2022, at which time we learned that the email account may have contained some of your personal or protected health information. As soon as we discovered that the incident impacted individual information, we immediately conducted a diligent search to identify current mailing addresses so that we could notify all potentially affected individuals.

Please note that this unauthorized access was limited to information transmitted via email and did not involve any other Centerstone information systems. We are not aware of the misuse of any personal or protected health information that may have been involved in this incident.

What Information Was Involved? The affected information may have included your <<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 you <<12/24 months>> of identity protection and credit monitoring services at no cost to you through IDX.

The IDX services include credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity 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 December 12, 2022.

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 1-833-764-0234 or by going to <https://app.idx.us/account-creation/protect> 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 information appears on the following page. If you have questions or need assistance, please call 1-833-764-0234, 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,

A handwritten signature in dark ink, appearing to read "D. Guth, Jr.", with a stylized flourish at the end.

David C. Guth, Jr.
Chief Executive Officer, Centerstone

Centerstone of Tennessee, Inc.
44 Vantage Way, Suite 400
Nashville, TN 37228

Additional Steps You Can Take to Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing 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 also should 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 (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 1-877-322-8228, 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 also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.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 one year. 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 for up to one year at no cost. 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. 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.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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