LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, TX 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

October 4, 2021

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

Re: Notice of Data Security Incident

To Whom It May Concern:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents The Menninger Clinic ("Menninger"), a psychiatric hospital located in Houston, Texas, in connection with a recent data security incident described in greater detail below. Menninger takes the protection of all information within its possession very seriously and has taken significant steps to help prevent a similar incident from occurring in the future.

1. **Nature of the Security Incident.**

On March 30, 2021, Menninger discovered unusual activity relating to one Menninger employee email account. Menninger immediately took steps to investigate the activity and to secure its email environment. Menninger also engaged a leading, independent cybersecurity firm to investigate what happened and to determine whether any Menninger information may have been impacted. Through this investigation, Menninger learned that certain Menninger employee email accounts were accessed without authorization. Menninger then engaged a cybersecurity firm to review the contents of the impacted email accounts likely to contain personal information. On July 26, 2021, Menninger learned that personal information belonging to certain current and former employees and patients was contained in the email accounts. Menninger then worked diligently to identify current address information to provide notification. That process was completed on September 16, 2021.

The potentially impacted information may have included individuals' names, Social Security numbers, driver's license numbers and other identification numbers, credit card and bank account numbers, dates of birth, medical record numbers, treatment information, billing/claims information,

patient account numbers, diagnosis or symptom information, health insurance information, prescription information, electronic signatures, and tax information.

2. Number of Maine Residents Affected.

Menninger notified three potentially affected Maine residents via first class U.S. mail on September 24, 2021 and offered them complimentary credit monitoring and identity theft protection services through IDX. A sample copy of the notification letter is included with this correspondence.

3. Steps Taken Relating to the Incident.

Menninger has taken steps in response to this incident to help prevent similar incidents from occurring in the future. Menninger has, for example, worked since discovering this incident with leading cybersecurity experts to enhance the security of its network environment, implemented two-factor authentication throughout its environment, blocked all network logons from outside of the United States, implemented procedures to flag and analyze suspicious network activity, implemented a secure e-mail encryption desktop plug-in to enable end-users to more easily send encrypted emails, implemented various features of the Proofpoint tool to further harden Menninger's networks, and conducted additional end-use training.

4. Contact Information.

Menninger remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact me at 214.722.7141 or via email at Lindsay.Nickle@lewisbrisbois.com.

Very truly yours,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Consumer Notification Letter

Menninger
Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

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

September 24, 2021

Re: Notice of Data Security Incident

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

I am writing to inform you of a recent incident experienced by The Menninger Clinic ("Menninger") that may have impacted your personal information. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened: On March 30, 2021, Menninger discovered unusual activity relating to one Menninger employee email account. Menninger immediately took steps to investigate the activity and to secure its email environment. Menninger also engaged a leading, independent cybersecurity firm to investigate what happened and to determine whether any Menninger information may have been impacted. Through the investigation, Menninger learned that certain Menninger employee email accounts were accessed without authorization. Menninger then engaged a cybersecurity firm to review the contents of the impacted email accounts likely to contain personal information. On July 26, 2021, Menninger learned that your personal information may have been impacted by the incident. Menninger then worked diligently to identify your current address information to provide you with notification of this incident. That process was completed on September 16, 2021.

Please note that this incident only potentially impacted information transmitted via email and did not affect any other information systems. Menninger's electronic health records system was not accessed or otherwise impacted by this incident. In addition, Menninger has no evidence to suggest that your personal information has been or will be misused.

What Information Was Involved: The information that may have been involved included your name, <<variable text>>.

What We Are Doing: As soon as Menninger learned of this incident, Menninger took the steps described above. In addition, Menninger implemented additional measures to enhance the security of its email environment in an effort to minimize the likelihood of a similar event occurring in the future. Furthermore, Menninger reported the incident to the Federal Bureau of Investigation, the Department of Homeland Security, and the Houston Police Department and will provide whatever assistance is requested to assist law enforcement in efforts to hold the perpetrator(s) of the incident accountable.

Menninger is also providing you with information regarding steps that you can take to help protect your information. In addition, as an added precaution, Menninger is offering you complimentary identity protection services through IDX, a data breach and recovery services expert. IDX is assisting Menninger with its response to this incident. Your services include <<12 or 24>> 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 the deadline to enroll in the services being offered to you is December 24, 2021.

What You Can Do: Although Menninger is not aware of the misuse of any information potentially impacted in connection with this incident, Menninger encourages you to review the recommendations on the following page to help protect your information. Menninger also encourages you to contact IDX with any questions and to enroll in the free identity protection services being offered to you by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8am to 8pm Central Time. IDX representatives are fully versed on the incident and can answer questions or concerns you may have regarding protection of your information.

For More Information: If you have any questions regarding this incident or would like assistance enrolling in the services offered, please call 1-833-903-3648, Monday through Friday from 8am to 8pm Central Time. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

The security of your information is a top priority for Menninger, and Menninger is committed to safeguarding your data. Menninger sincerely apologizes for any inconvenience that this matter may cause.

Sincerely,

Armando E. Colombo
President & Chief Executive Officer
The Menninger Clinic

STEPS YOU CAN TAKE TO HELP 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 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:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report with the three credit bureaus. An initial fraud alert is free and will stay on your credit file for 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 or changing your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. To place a fraud alert on your credit report, contact one of the credit reporting agencies. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, 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
http://www.consumer.ftc.gov and www.ftc.gov/idtheft
1-877-438-4338

Maryland AG	**New York AG**	**North Carolina AG**	**Oregon AG**	**Rhode Island AG**
200 St. Paul Place Baltimore, MD 21202 http://www.oag.state.md.us 1-888-743-0023	The Capitol Albany, NY 12224 http://www.ag.ny.gov 1-800-771-7755	9001 Mail Service Center Raleigh, NC 27699 http://www.ncdoj.gov 1-877-566-7226	1162 Court Street NE Salem, OR 97301 http://www.doj.state.or.us 1-877-877-9392	150 South Main Street Providence, RI 02903 http://www.riag.ri.gov 401-274-4400

California Residents: Visit the California Office of Privacy Protection (http://www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Law Enforcement: You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Menninger
Return to IDX
10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-833-903-3648
Or Visit:
https://app.idx.us/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

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

September 24, 2021

Re: Notice of Data Security Incident

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

I am writing to inform you of a recent incident experienced by The Menninger Clinic ("Menninger") that may have impacted your personal information. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

What Happened: On March 30, 2021, Menninger discovered unusual activity relating to one Menninger employee email account. Menninger immediately took steps to investigate the activity and to secure its email environment. Menninger also engaged a leading, independent cybersecurity firm to investigate what happened and to determine whether any Menninger information may have been impacted. Through the investigation, Menninger learned that certain Menninger employee email accounts were accessed without authorization. Menninger then engaged a cybersecurity firm to review the contents of the impacted email accounts likely to contain personal information. On July 26, 2021, Menninger learned that your personal information may have been impacted by the incident. Menninger then worked diligently to identify your current address information to provide you with notification of this incident. That process was completed on September 16, 2021.

Please note that this incident only potentially impacted information transmitted via email and did not affect any other information systems. Menninger's electronic health records system was not accessed or otherwise impacted by this incident. In addition, Menninger has no evidence to suggest that your personal information has been or will be misused.

What Information Was Involved: The information that may have been involved included your name, <<variable text>>.

What We Are Doing: As soon as Menninger learned of this incident, Menninger took the steps described above. In addition, Menninger implemented additional measures to enhance the security of its email environment in an effort to minimize the likelihood of a similar event occurring in the future. Furthermore, Menninger reported the incident to the Federal Bureau of Investigation, the Department of Homeland Security, and the Houston Police Department and will provide whatever assistance is requested to assist law enforcement in efforts to hold the perpetrator(s) of the incident accountable.

Menninger is also providing you with information regarding steps that you can take to help protect your information. In addition, as an added precaution, Menninger is offering you complimentary identity protection services through IDX, a data breach and recovery services expert. IDX is assisting Menninger with its response to this incident. Your services include <<12 or 24>> 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 the deadline to enroll in the services being offered to you is December 24, 2021.

What You Can Do: Although Menninger is not aware of the misuse of any information potentially impacted in connection with this incident, Menninger encourages you to review the recommendations on the following page to help protect your information. Menninger also encourages you to contact IDX with any questions and to enroll in the free identity protection services being offered to you by calling 1-833-903-3648 or going to https://app.idx.us/account-creation/protect and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 8am to 8pm Central Time. IDX representatives are fully versed on the incident and can answer questions or concerns you may have regarding protection of your information.

For More Information: If you have any questions regarding this incident or would like assistance enrolling in the services offered, please call 1-833-903-3648, Monday through Friday from 8am to 8pm Central Time. You will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

The security of your information is a top priority for Menninger, and Menninger is committed to safeguarding your data. Menninger sincerely apologizes for any inconvenience that this matter may cause.

Sincerely,

Armando E. Colombo
President & Chief Executive Officer
The Menninger Clinic

STEPS YOU CAN TAKE TO HELP 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 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:

TransUnion	**Experian**	**Equifax**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374
1-800-916-8800	1-888-397-3742	1-888-548-7878
www.transunion.com	www.experian.com	www.equifax.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report with the three credit bureaus. An initial fraud alert is free and will stay on your credit file for 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 or changing your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. To place a fraud alert on your credit report, contact one of the credit reporting agencies. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: Under U.S. law, 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
http://www.consumer.ftc.gov and www.ftc.gov/idtheft
1-877-438-4338

Maryland AG	**New York AG**	**North Carolina AG**	**Oregon AG**	**Rhode Island AG**
200 St. Paul Place	The Capitol	9001 Mail Service Center	1162 Court Street NE	150 South Main Street
Baltimore, MD 21202	Albany, NY 12224	Raleigh, NC 27699	Salem, OR 97301	Providence, RI 02903
http://www.oag.state.md.us	http://www.ag.ny.gov	http://www.ncdoj.gov	http://www.doj.state.or.us	http://www.riag.ri.gov
1-888-743-0023	1-800-771-7755	1-877-566-7226	1-877-877-9392	401-274-4400

California Residents: Visit the California Office of Privacy Protection (http://www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Law Enforcement: You have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf