BASS Medical Group Notifies Individuals of Data Security Incident

Walnut Creek, CA – October 22, 2026 – BASS Medical Group ("BASS") is providing notice of a recent data security incident that may have involved personal and/or protected health information. BASS takes the privacy and security of all information within our possession very seriously. BASS is providing this notification to notify potentially involved individuals about this incident.

On or around September 4, 2026, BASS discovered suspicious activity within its network environment. Upon discovery, we immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to identify the source and scope of the incident. On or about September 22, 2026, the investigation determined that certain personal and/or protected health information may have been accessed or acquired without authorization.

Based on BASS's review of the potentially affected data set, the following information may have been involved as a result of the incident: medical treatment codes or billing information and health insurance information. Not all information was involved for all individuals. **We currently have no evidence to suggest misuse or attempted misuse of this information.**

As soon as we discovered the incident, we took the steps described above and implemented additional safeguards to help ensure the security of its systems and reduce the risk of a similar incident occurring in the future.

In addition, we have established a toll-free call center to answer questions about the incident and address related concerns. The call center is available Monday through Friday from 5:00 a.m. – 5:00 p.m. Pacific Time, excluding major U.S. holidays, and can be reached at 1-855-711-7083. We also notified the California Attorney General, the FBI, and the U.S. Health and Human Services Office for Civil Rights of this incident.

The privacy and security of any information in our possession is of utmost importance to BASS, and we deeply regret any concern or inconvenience this incident may cause.

BASS is providing the following information to help those wanting to know more about steps they can take to protect themselves and their information:

What steps can I take to protect my 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 the three major credit reporting agencies 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 105069, Atlanta, GA 30348, 1-800-525-6285, www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
- *Experian*, P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, https://www.experian.com/help/fraud-alert/
- *TransUnion*, P.O. Box 2000, Chester, PA 19016, 1-800-916-8800, www.transunion.com/fraud-alerts

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 and

requires them to take steps to verify your identity before extending new credit. To place a fraud alert, you only need to contact one of the three credit reporting agencies identified above. The agency you contact is required to notify the other two agencies to place fraud alerts on your credit files. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file at no cost. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent, which can help prevent new credit accounts from being opened in your name without authorization. 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. To find out more on how to place a security freeze, you can use the following contact information:

- *Equifax Security Freeze*, P.O. Box 105788, Atlanta, GA 30348, 1-888-298-0045, www.equifax.com/personal/credit-report-services/credit-freeze/
- *Experian Security Freeze*, P.O. Box 9554, Allen, TX 75013, 1-888-397-3742, www.experian.com/freeze
- *TransUnion Security Freeze*, P.O. Box 160, Woodlyn, PA 19094, 1-800-916-8800, www.transunion.com/credit-freeze

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. Please visit https://www.consumerfinance.gov/consumer-tools/credit-reports-and-scores/answers/key-terms/ to learn more.

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-reportingact.pdf or https://www.consumerfinance.gov/learnmore/.