

### **NOTICE OF DATA PRIVACY INCIDENT**

HPHG, LLC d/b/a 90 Degree Benefits, San Antonio ("90 Degree Benefits, San Antonio") 90 Degree Benefits, San Antonio is committed to the privacy and security of the information in its possession. Out of an abundance of caution, 90 Degree Benefits, San Antonio is notifying potentially impacted individuals to inform them of this incident and steps individuals can take to help safeguard their information.

In September 2024, 90 Degree Benefits, San Antonio identified suspicious activity related to an employee email account. Upon learning of the activity, 90 Degree Benefits, San Antonio immediately took steps to secure the account and launched an investigation into the nature and scope of the event. The investigation determined that an unauthorized actor gained access to the email account between September 17, 2024 and September 18, 2024 and that certain emails and/or attachments were also accessed. As part of the investigation, 90 Degree Benefits, San Antonio conducted a review of the involved emails to determine what information was within them and to whom the information relates. This determined that the information for certain client plan participants may have included names, health insurance identification numbers, patient identification numbers, provider information, and/or billing and claims information. The incident **did not** involve Social Security numbers or financial account information.

As a result, on January 17, 2025, 90 Degree Benefits, San Antonio began notifying impacted customer covered entities whose plan participant information was potentially involved, including an offer to provide notification to plan participants directly on behalf of the impacted clients.

The confidentiality, privacy, and security information in our care are among our highest priorities. To reduce the risk of a similar event from occurring again, 90 Degree Benefits, San Antonio has taken several actions to further secure its email environment, including reviewing relevant processes and procedures and providing additional training to employees.

As a general precaution, 90 Degree Benefits, San Antonio encourages potentially involved individuals to remain vigilant against the potential for identity theft and fraud and to monitor their accounts, medical bills, explanation of benefits forms, and credit reports for any suspicious activity and to detect errors.

If you have further questions, or believe you may be impacted by this event, please contact 888-267-4445, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time, excluding major U.S. holidays. Our representatives are fully versed on this incident and can help answer questions you may have regarding the protection of your information.

#### **General Information**

90 Degree Benefits, San Antonio encourages everyone to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and explanation of benefits and monitoring your free credit reports for suspicious activity and to detect errors. If you detect any suspicious activity on your 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").

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:

<b>Equifax</b>	<b>Experian</b>	<b>TransUnion</b>
P.O. Box 105851 Atlanta, GA 30348 1-800-525-6285	P.O. Box 9532 Allen, TX 75013 1-888-397-3742	P.O. Box 2000 Chester, PA 19016 1-800-799-5355

You have the right to place a “security freeze” on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed above.

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, [www.identitytheft.gov](http://www.identitytheft.gov), 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade

Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.