<<LOGO>>

[address]

<<Mail ID>>
<<Name 1>> <<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>>, <<State>> <<Zip>>

[Date]

Re: Notice of Data Breach

Dear <<Name 1>>:

Pacific Symphony is notifying you of a cybersecurity incident that may have involved your personal information

What happened. On August 21, 2025, Pacific Symphony was alerted to an unauthorized third-party accessing part of Pacific Symphony's IT network. Our IT team responded promptly, taking immediate steps to terminate the unauthorized access and resecure the network.

What we are doing in response. Third-party cybersecurity experts were engaged promptly, and a comprehensive investigation was launched to determine the scope and potential impact of the event. The preliminary results from the investigation did not find evidence that any sensitive personal information was affected. The investigation later determined that the unauthorized third-party had the opportunity to extract data from a limited part of our IT environment. We then conducted an extensive document review process, which involved hand reviewing individual documents, to identify individuals who potentially needed to be notified of this incident.

What information was involved. Our review found the following information for you in the potentially affected files: your full name, <<NPPI Letter Text for data elements>>.

What you can do. While we have no evidence that any personal information has actually been used inappropriately, we recommend you take precautions, and **we are offering you 12 months of *free* credit monitoring and $1 million in identity theft insurance through Experian - to give you peace of mind. *You must activate the free product by the activation date in order for it to be effective*. *The activation instructions are included with this notification.*** We also encourage you to activate two-factor authentication (with prompting via text or email) for your online accounts. If this letter indicates that your bank account information may have been affected, we also recommend speaking with your bank about obtaining a new account number. Also included are some additional steps that you can take to protect yourself, as you deem appropriate.

For more information about this incident, call <<phone number>> between 9:00 am - 5:30 pm PST Monday - Friday (excluding holidays). Pacific Symphony is continuing to take steps to enhance its security measures to help prevent something like this from happening in the future. We are fully committed to protecting your personal information and sincerely apologize for any concern this incident may cause you.

Sincerely,

Pacific Symphony

STEPS YOU CAN TAKE

Below is information about steps you can take to protect yourself if you feel this is necessary or appropriate.

- **ACTIVATE Your FREE Experian IdentityWorks Product NOW in Three Easy Steps.** To help protect your identity, we are offering you a **complimentary membership** of Experian's ***IdentityWorks*** product for **12 months**. This product helps detect possible future misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. IdentityWorks Alert is completely free to you and enrolling in this program will not hurt or impact on your credit score.

  1. **ENSURE You Enroll By**: << activation deadline>> **(Your code will not work after this date.)**

  2. **VISIT** the **Experian IdentityWorks website** to enroll: <<URL>> **PROVIDE Your Activation Code**: **<<activation code>>**

  If you have questions about the IdentityWorks or need an alternative to enrolling online, **please call 877-288-8057** and provide engagement **<engagement number>>.** A credit card is not required for enrollment. Once your IdentityWorks membership is activated, you will receive the following features:

  - **Experian Credit Report at Signup:** See what information is associated with your credit file. Daily credit reports are available for online members only. [1]
  - **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
  - **Identity Restoration:** Restoration Agents are immediately available to help address credit/non-credit related fraud.
  - **$1 Million Identity Theft Insurance:** [2] Provides coverage for certain costs and unauthorized electronic fund transfers.

  You must activate your membership by the Enrollment Date (noted above) by enrolling at https://www. <<URL>> or calling 877-288-8057 to register the activation code above in order for this service to be activated. Once your enrollment in IdentityWorks is complete, carefully review your credit report for inaccurate or suspicious items. If you have any questions about IdentityWorks, need help understanding something on your credit report, or suspect that an item on your credit report may be fraudulent, please contact Experian's customer team at 877-288-8057.

ADDITIONAL STEPS YOU MAY WISH TO TAKE

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS & REPORT FRAUD AND IDENTITY THEFT**. **CHANGE PASSWORDS AND SECURITY VERIFICATION QUESTIONS & ANSWERS.** It is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements for unauthorized activity– especially over the next 24 months. Activate alerts on your bank accounts to notify you of suspicious activity and change passwords/security verifications as needed – particularly if same the password is used over multiple online accounts. If your medical information was involved and referenced in this notice, it is also advisable to review the billing statements you receive from your healthcare providers.

---

[1] Offline members will be eligible to call for additional reports quarterly after enrolling.

[2] The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Immediately report suspicious activity, fraudulent charges, or suspected identity theft related to your insurance statements, provider billing statements, credit report, credit card or bank accounts to your insurance company, bank/credit card vendor, healthcare provider, and law enforcement, including FTC and/or your State Attorney General.

- **FREEZE YOUR CREDIT FILE.** You have a 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 expressed authorization. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, using a freeze to take control over who gets access to the personal/financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application made regarding a new loan, credit, mortgage, or any other account involving extension of credit. A security freeze generally does not apply to existing account relationships or when a copy of your report is requested by an existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. It is free to place, lift, or remove a security freeze – which can be done quickly and easily. To place a security freeze on your credit report, contact each of the following credit bureaus and clearly explain in the call/letter that you are requesting a security freeze, or you can usually do so online:

  - *Equifax*, PO Box 105788, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
  - *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
  - *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

  To request a security freeze, provide your full name (middle initial, Jr., Sr., II, III, etc.), Social Security Number, date of birth; home addresses over the past 5 years; proof of current address such as a current utility bill or telephone bill; photocopy of government issued identification card (driver's license or ID card, military ID, etc.); and 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. If you request a security freeze via toll-free telephone or other secure electronic means, credit reporting agencies have 1 business day after receiving the request to place the freeze. In the case of a request made by mail, the agencies have 3 business days after receiving your request to place a security freeze on your credit report. Credit agencies must also send written confirmation within 5 business days and provide a unique personal identification number (PIN) or password, or both that can be used to authorize the removal or lifting of the security freeze. To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and PIN or password provided when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have 3 business days after receiving a request to lift the freeze for those identified entities or for the specified period of time. To remove the freeze, you must send a written request to the 3 credit bureaus by mail and include proper identification (name, address, & social security number) and PIN number or password provided when you placed the freeze. The credit bureaus have 3 business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 an alert lasting 7 years. Contact the 3 credit reporting agencies listed above to activate an alert.

- **ORDER FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-

322-8228 to obtain 1 free copy of your credit report annually. Periodically review a copy of your credit report for discrepancies and identify accounts you did not open or inquiries you did not authorize. For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) copies of your credit report, free of charge. You must contact each of the 3 credit reporting agencies directly to obtain such additional reports.

- *Equifax*, PO Box 105281, Atlanta, GA 30348, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

- **SUMMARY OF YOUR RIGHTS UNDER FAIR CREDIT REPORTING ACT (FCRA):** FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552. (1) You must be told if information in your file has been used against you. (2) You have the right to know what is in your file. (3) You have the right to ask for a credit score. (4) You have the right to dispute incomplete or inaccurate information. 5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. (6) Consumer reporting agencies may not report outdated negative information. (7) Access to your file is limited. (8) You must give your consent for reports to be provided to employers. (9) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. (10) You have a 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. (11) You may seek damages from violators. (12) Identity theft victims and active-duty military personnel have additional rights.

- **CONTACT LAW ENFORCEMENT AND FEDERAL TRADE COMMISSION (FTC.** If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement and the FTC. You may also contact these agencies for information on fraud alerts and security freezes and how to prevent or minimize the risks of identity theft. You may contact the FTC at www.ftc.gov/idtheft; FTC hotline is 877-438-4338; TTY: 1-866-653-4261 or write to FTC, 600 Pennsylvania Ave., NW, Washington, D.C. 20580.