<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<Date>> (Format: Month Day, Year)

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

NOTICE OF DATA BREACH

Dear <<First_name>> <<Last_name>>:

I am writing on behalf of Phreesia, Inc. ("Phreesia"), a company that helps healthcare organizations automate their patient check-in processes and other administrative functions. Phreesia was the victim of a recent security incident that may have involved some of your personal information, which we received as part of providing services to your healthcare provider. While we are unaware of any attempted or actual misuse of any information involved in this incident, we are sending this letter to explain what happened, what we have done in response, and what steps you can take to protect against misuse of your personal information. We regret that this occurred and take the security of personal information seriously.

WHAT HAPPENED. On August 25, 2025, Phreesia learned that it was among the many organizations impacted by a security incident involving a third-party software tool called Salesloft Drift. An unknown third party exploited a previously unknown vulnerability in that software tool and accessed the Salesforce environments of hundreds of organizations, including ours. The vulnerability that was exploited was not in Phreesia's systems and the incident *only* affected the Salesforce environment that we use to store information shared by healthcare organizations when they ask for help resolving customer service issues. These service tickets occasionally include small amounts of patient information where relevant to fixing the issue.

Upon learning of the incident, we immediately took steps to secure our Salesforce environment, including turning off Salesloft Drift. We also launched an investigation, with support from external cybersecurity experts, to assess the impact of the incident on our environment or data. Through this investigation, we determined that, on August 17, 2025, the unknown third party had access to service tickets in Salesforce, which in some cases included limited patient information

WHAT INFORMATION WAS INVOLVED. You are receiving this notice because your information was identified within the Salesforce environment. We have determined that the personal information involved in this incident may have included your <<b2b_text_1 (Data Elements)>><<b2b_text_2 (Data Elements continued)>>. Please note that the unauthorized third party did not have access to your medical chart, payment card or financial account information. The incident was limited to service tickets within the Salesforce environment.

WHAT WE ARE DOING. After becoming aware of the incident, Phreesia immediately stopped using the affected software and took steps to confirm that the incident was contained. Phreesia also worked with external cybersecurity experts to determine the full nature and scope of the incident and identify any impacted information. We have also taken steps designed to prevent something like this from happening again, including adding new security measures and reviewing our third-party risk management practices.

WHAT YOU CAN DO. We are not aware of any misuse of your personal information. However, consistent with certain laws, we are providing you with the enclosed information, "Steps You Can Take to Help Protect Your Information."

As a precaution, we have arranged for you, at your option, to enroll in a complimentary two-year identity and credit monitoring service, provided by Kroll. Your identity monitoring services include credit monitoring, fraud consultation, and identity restoration services.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until *<<b2b_text_6 (activation deadline)>>* to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

This code is unique for your use and should not be shared.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us at (844) 572-2754 if you have any questions or concerns.

Sincerely,

Evan Roberts
President, Provider Solutions | Phreesia, Inc.

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institutions.

OBTAIN A FREE CREDIT REPORT. You may also periodically obtain credit reports from the nationwide credit reporting agencies. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.Equifax.com

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.Experian.com

TransUnion
(800) 680-7289
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
www.TransUnion.com

PLACE A FRAUD ALERT OR SECURITY FREEZE. You also have other rights under the Fair Credit Reporting Act (FCRA). For information about your rights under the FCRA, please visit: https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the Federal Trade Commission (FTC) and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to verify your identity. You may place a fraud alert in your file by calling any of the nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze to restrict access to your credit report. You will need to provide the credit reporting agency with certain information, such as your name, address, date of birth, and Social Security Number. After receiving your request, the credit reporting agency will send you a confirmation containing a unique PIN or password that you will need in order to remove or temporarily lift the freeze. You should keep the PIN or password in a safe place.

ADDITIONAL INFORMATION. In addition, you may contact the Federal Trade Commission (FTC) or law enforcement, including your state attorney general, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's website at www.ftc.gov/idtheft, or call the FTC at (877) IDTHEFT (438-4338) or write to Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

State-Specific Information

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may obtain information about avoiding identity theft from the FTC or the District of Columbia Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

Office of the Attorney General
400 6th Street, NW
Washington, DC 20001
(202) 727-3400
www.oag.dc.gov/

IF YOU ARE AN IOWA RESIDENT: You may contact local law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft.

Office of the Attorney General of Iowa
Consumer Protection Division
Hoover State Office Building
1305 E. Walnut Street
Des Moines, IA 50319
(515) 281-5926
www.iowaattorneygeneral.gov/

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the FTC or the Maryland Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
www.marylandattorneygeneral.gov/

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the FTC or from the following New York state agencies:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

New York Attorney General
The Capitol
Albany, NY 12224
(800) 771-7755
www.ag.ny.gov

New York Department of State
Division of Consumer Protection
99 Washington Avenue
Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the FTC or the North Carolina Attorney General's Office. These offices can be reached at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
(877) IDTHEFT (438-4338)
www.consumer.ftc.gov/idtheft

North Carolina Department of Justice
Attorney General Jeff Jackson
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
www.ncdoj.gov

IF YOU ARE A RHODE ISLAND RESIDENT: We have determined that the incident involved personal information regarding 18 Rhode Island individuals. You may contact state or local law enforcement to determine whether you can file or obtain a police report relating to this incident. In addition, you can contact the Rhode Island Attorney General at:

Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
www.riag.ri.gov/