PRIMIS

Return to IDX:
P.O. Box 989728
West Sacramento, CA 95798-9728

Enrollment Code: <<Enrollment Code>>

To Enroll, Scan the QR Code Below:

SCAN ME

Or Visit:
https://response.idx.us/primisbank

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

August 24, 2023

Subject: Notice of Third-Party Data <<Variable Text 1 – Breach or Security Incident>>

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

Primis Bank ("Primis") is writing to inform you of a recent third-party data security incident that may have affected your personal information. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened? On July 24, 2023, Darling Consulting Group ("Darling") advised Primis that it was recently affected by the MOVEit software vulnerability. Darling provides analytical services for various companies and organizations, including Primis, and utilizes the MOVEit tool to transfer data to and from its clients. The MOVEit vulnerability has impacted an estimated 2,500 companies and other organizations worldwide, including universities and government agencies, and resulted in the exposure of personal information of millions of customers.

Primis' systems were not compromised. Per Darling, the MOVEit vulnerability resulted in files pertaining to Primis being downloaded from Darling's systems by an unauthorized actor between May 30 and May 31, 2023. Primis thereafter undertook a review of the potentially affected files and identified personal information for certain individuals therein.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name and <<Variable Text 2 – Data Elements>>.

What Are We Doing? As soon as we learned of the incident, Primis conducted a detailed review of the impacted files to determine whether any individuals' information was involved. Primis then arranged to provide formal notification to affected individuals as quickly as possible. We understand that Darling took remediation measures as directed by the MOVEit software developer and will be evaluating alternative file sharing platforms moving forward. Additionally, Primis will be evaluating additional safeguards that can be put in place to enhance the security of information transmitted externally by Primis.

In addition, Primis is offering complimentary identity theft protection services through IDX – a data breach and recovery services expert. IDX identity protection services include: <<12/24>> months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. We also encourage you to take advantage of the complimentary identity protection services being offered through IDX by calling 1-888-901-6462 or going to https://response.idx.us/primisbank, or scanning the QR image and

using the Enrollment Code provided above. If you have questions about the enrollment process or need assistance enrolling, IDX representatives are available Monday through Friday from 9:00 am – 9:00 pm Eastern Time. Please note the deadline to enroll is November 24, 2023.

For More Information: To help answer any questions regarding this incident, Primis has established a dedicated call center through IDX. The call center can be reached at 1-888-901-6462 Monday through Friday from 9:00 am – 9:00 pm Eastern Time. IDX representatives are well-versed in the incident and can answer any questions you may have.

Please be assured that Primis takes the privacy and security of personal information very seriously. Even though the compromised systems belong to a vendor and not Primis, we hope you will accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Dennis J. Zember Jr.
President & CEO

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 incidents 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 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 105851
Atlanta, GA 30348
1-800-525-6285

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800

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 within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

Security Freeze: 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
consumer.ftc.gov
1-877-438-4338

Maryland Attorney General
St. Paul Plaza
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
ag.ny.gov
1-212-416-8433 / 1-800-771-7755

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
400 S 6th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

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