



IDX Return Address:
4145 SW Watson Ave
Suite 400
Beaverton, OR 97005

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

April 17, 2023

Subject: Notice of Data <<Variable Text 1: Breach or Security Incident>>

Dear <<First Name>> <<Last Name>>:

I am writing to inform you of a recent data security incident experienced by NewBridge Services (“NewBridge”) that may have affected your personal and protected health information. NewBridge takes the privacy and security of all information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened? On January 26, 2023, NewBridge discovered that it had experienced an incident disrupting access to certain of its systems. In response, NewBridge took immediate steps to secure its systems and promptly launched an investigation. In so doing, NewBridge engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On January 28, 2023, NewBridge learned that your personal and protected health information may have been impacted in connection with the incident which is the reason for this notification. Please note that NewBridge has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your name and <<Variable Text 2: Potentially Impacted Data Sets>>.

What Are We Doing? As soon as NewBridge discovered this incident, it took the steps described above. In addition, NewBridge implemented measures to enhance the security of its digital environment in an effort to minimize the risk of a similar incident occurring in the future. NewBridge also notified the Federal Bureau of Investigation of this incident and will provide whatever cooperation is necessary to hold the perpetrator(s) of the incident accountable.

Although NewBridge has no evidence of the misuse of any potentially impacted information, NewBridge is providing you with information about steps that you can take to help protect your personal and protected health information.

What You Can Do: You can follow the recommendations on the following page to help protect your personal and protected health information.

For More Information: Further information about how to protect your personal and protected health information appears on the following page. If you have questions, please call 1-833-903-3648 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). Call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that NewBridge takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Michelle Borden, MSW, LCSW

Michelle Borden, MSW, LCSW
Chief Executive Officer
NewBridge Services, Inc.
7 Industrial Road
Pequannock, NJ 07840

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 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 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
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

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, and
www.ftc.gov/idtheft
1-877-438-4338

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

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

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-reporting-act.pdf>.