

August [X], 2016

Newkirk Products, Inc.
PO Box 62939
El Dorado Hills CA 95762-9039

Dear [Member Name],

Newkirk Products, Inc. (“Newkirk” or “we”), a service provider that issues healthcare ID cards for your prescription drug plan, Symphonix Health, had a cyber security incident that may affect your personal information.

What Happened?

On July 6, 2016, Newkirk discovered a server containing member information was accessed without authorization. We shut down the server and started an investigation into the incident. The server did **not** include Social Security numbers, banking or credit card information, medical information or any insurance claims information. We hired a third-party forensic investigator to determine the extent of the unauthorized access and whether the personal information of our clients’ members may have been accessed. We also notified federal law enforcement. While the forensic investigation is ongoing, it appears the unauthorized access first occurred on May 21, 2016. Although the information contained on the server may have been accessed, Newkirk has no evidence to date that data has been used inappropriately.

Please be advised that Symphonix Health’s systems were not accessed or affected in any way.

What Information Was Involved?

The information potentially accessed consists of your name, mailing address, date of birth, type of plan, member and group ID number, plan effective date, premium information, deductible and copayment amounts, and other information found on your ID card. To date, we have no evidence that your personal information has been misused.

Why Does Newkirk Have Your Information?

We had your personal information as we were contracted to create your health insurance ID cards.

What We Are Doing

In an abundance of caution, we are offering two years of identity protection and restoration services with AllClear ID at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next two years.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-303-9773 (TTY/TDD: 711) and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Identity Theft Monitoring: This service offers additional layers of protection including identity theft monitoring that delivers secure, actionable alerts to you by phone and \$1 million identity theft insurance coverage. To use this service, you will need to provide your personal information to AllClear ID. You may sign up online at newkirkproductsfacts.allclearid.com. Please note: Additional steps may be required by you in order to activate your phone alerts and monitoring options.

In addition, we are taking measures to improve our cyber security controls to help reduce the risk of this type of incident occurring again.

What You Can Do

While the information potentially accessed was limited, we encourage you to enroll with AllClear ID. You can also review the enclosed Additional Resources and Helpful Information. We also encourage you to be vigilant against incidents of identity theft or medical benefit fraud. You can do this by reviewing your account statements, medical bills, and health insurance Explanation of Benefits statements regularly for suspicious activity. Report all suspicious or fraudulent charges to Symphonix Health.

For More Information

Newkirk recognizes this issue is concerning to you and we are taking steps to help protect you. Should you have any questions regarding this incident, please visit www.newkirkproductsfacts.com or call the AllClear ID dedicated call center we have set up regarding this incident at 1-855-303-9773 (TTY/TDD: 711) between Monday - Saturday, 8am - 8pm Central Time. This notice is available in other formats for members with special needs. Oral translation is an option for members who speak languages other than English and Spanish.

Newkirk takes your privacy and the security of your protected health information seriously. We sincerely regret any inconvenience or concern this incident causes you.

Sincerely,

[Name]

[Title]

*Newkirk Products, Inc. was acquired by Broadridge Financial Solutions, Inc. on July 1, 2016.

Additional Resources and Helpful Information

Although your Social Security number was not exposed, there are some steps that you can take to protect yourself from identity theft generally. Here are recommendations from experts on identity protection.

- **Visit the Federal Trade Commission's Identity Theft Website**

To learn about the steps you can take to avoid identity theft, visit the Federal Trade Commission's website at <http://www.ftc.gov/bcp/edu/microsites/idtheft/>.

You can also contact the FTC via phone at 1-877-ID-THEFT (877-438-4338) or via mail to the FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

- **Check your credit reports annually**

We recommend that you check all of your consumer reports annually. You may obtain a free copy of your credit report once every 12 months from each of the nationwide consumer reporting agencies by visiting <http://www.annualcreditreport.com> or by contacting the consumer reporting agencies at:

Equifax (800) 685-1111 P.O. Box 740256 Atlanta, GA 30374 www.equifax.com	Experian (888) 397-3742 P.O. Box 2002 Allen, TX 75013 www.experian.com	TransUnion (800) 916-8800 P.O. Box 2000 Chester, PA 19022-2000 www.transunion.com
---	--	---

- **Consider Placing a Fraud Alert**

You may wish to place a fraud alert on your credit report. The fraud alert is a consumer statement that alerts creditors of possible fraudulent activity within your report as well as requests that they contact you prior to establishing any accounts in your name. Once the fraud alert is added to your credit report, all creditors should contact you prior to establishing any account in your name.

There are also two types of fraud alerts that you can place on your credit report: an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies listed below.

Equifax:	1-888-766-0008
Experian:	1-888-397-3742
TransUnion:	1-800-680-7289

- **Consider a Security Freeze**

A security freeze prevents a consumer reporting agency from releasing your credit report without your authorization. . However, using a security freeze may delay your ability to obtain credit. You may request that a freeze be placed on your consumer report by sending a written request to each credit reporting agency by certified mail, overnight mail or regular stamped mail to the address below.

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

TransUnion (FVAD)
P.O. Box 2000
Chester, PA 19022-2000

The following information should be included when requesting a security freeze: full name, with middle initial and any suffixes; Social Security number; full date of birth; current address and previous addresses for the past two years. The request also should include a copy of a government-issued identification card, such as a driver's license, state or military ID card, and a copy of a recent utility bill, bank or insurance statement that verifies your current residence.

The consumer reporting agency may charge a fee to place a freeze or lift or remove a freeze, unless you are a victim of identity theft and have submitted a police report to the consumer reporting company.

Each credit reporting agency will send a written confirmation to you regarding the freeze along with a unique personal identification number (PIN) that can be used by you to authorize the removal or lifting of the security freeze. It is very important for you to protect and remember the PIN. To lift the security freeze in order to allow a specific entity or individual access to your credit report or to remove the freeze, you must contact the credit reporting agencies and provide your identification information and the PIN.

You can also place, lift or remove a security freeze using these websites:

Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp

Experian: <https://www.experian.com/freeze/center.html>

TransUnion: <https://www.transunion.com/credit-freeze/place-credit-freeze>

ADDITIONAL INFORMATION FOR CERTAIN STATE RESIDENTS

CALIFORNIA: The mailing of this notice was not delayed by law enforcement. You can obtain additional information from the California Office of Privacy Protection (www.privacy.ca.gov) on protection against identity theft.

CONNECTICUT: You have the right to place a security freeze on your consumer reports. Please see the information about placing a security freeze above.

RHODE ISLAND: You have the right to file a police report. You also have the right to place a security freeze on your consumer reports. Please see the information about placing a security freeze above. Rhode Island residents may contact the Office of the Attorney General for more information about identity theft: Rhode Island Office of the Attorney General - <http://www.riag.ri.gov/>, 150 South Main Street, Providence, RI 02903.

WYOMING: The mailing of this notice was not delayed by law enforcement.