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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Re: Notice of Data Breach from MultiPlan

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

MultiPlan Inc., a vendor that provides medical payment billing services to Highmark Inc., takes the privacy and security of the information it handles very seriously. Unfortunately, on behalf of Highmark, we at MultiPlan must notify you of an incident that may have impacted your information.

What happened?

On January 27, 2021, MultiPlan identified a security matter involving unauthorized access to one of our employee's email accounts by an outside bad actor. Upon discovering the incident, we immediately terminated the unauthorized access, changed the employee's credentials, and an investigation supported by forensics experts was commenced to determine what happened. The matter was also reported to law enforcement. The investigation concluded that the goal of the outside actor was to divert wire payments from a small number of customers seeking to pay invoices to the vendor. In the process of carrying out this attempt the outside actor had access to the employee's email account, which was used to communicate with Highmark regarding billing, and within those communications was some information about your account.

What information was involved?

Please be assured that this matter did not involve Highmark's network or systems in any way. This matter only affected one email account belonging to MultiPlan. While it does not appear that individual member information was the target of this incident, we cannot say with certainty which emails or attachments may have been accessed or acquired by the outside actor and so out of an abundance of caution, we are notifying you that your personal information may have been involved and between December 23, 2020 and January 27, 2021, the following information could have been accessed or acquired: <<b2b_text_2(ImpactedData)>>.

What we are doing:

In addition to providing you with this notice, we have arranged for you to receive an offer of credit monitoring at no cost to you for a period of two years. To accept this offer, please follow the instructions in the attachment.

Your credit monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **October 7, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

Additional information describing your services is included with this letter.

MultiPlan has also taken actions to reinforce its existing security protocols and processes to reduce the likelihood of this situation occurring in the future including reinforcing email authentication requirements, providing additional training to employees and increasing phishing campaign training. Additionally, MultiPlan has engaged a third party security firm to conduct a thorough analysis of our information security policies, procedures and controls and we will implement any relevant, suggested enhancements..

What you can do:

We are not aware of any misuse of your information. However, it is always a good practice to remain vigilant and regularly review your financial statements, credit reports, and Explanations of Benefits (EOBs) from your health insurers for any unauthorized activity. If you identify suspicious activity, you should contact the company that maintains the account on your behalf.

Additional information about protecting your identity is attached to this notice.

For more information:

If you have questions, please call 1-XXX-XXX-XXXX Monday through Friday from 9:00am to 6:30pm Eastern Time.

We regret that this incident occurred, and we want to assure you again that we take the privacy and security of your information very seriously.

Sincerely,

MultiPlan

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

*You have until **October 7, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit.

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

California Residents: Visit the California Office of Privacy Protection (https://oag.ca.gov/privacy) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; +1 (888) 743-0023; or www.oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9332 (toll-free in Oregon), +1 (503) 378-4400, www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, RI 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.