



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

<<<b2b\_text\_1 (Re: Notice of Data [Breach / Security Incident])>>

Dear <<first\_name>> <<last\_name>>:

The Phia Group, LLC (“The Phia Group”) is writing to notify you of a data security incident which may have affected the privacy of your information. The Phia Group works with health benefit plans and their third-party administrators, and is an experienced provider of healthcare cost containment techniques designed to control healthcare and benefit plan costs. We held limited information related to you due to our relationship with <<b2b\_text\_2 (Client)>>. Phia takes the privacy and security of information in its possession very seriously and sincerely apologizes for any inconvenience this incident may cause. Please read this letter carefully as it contains information regarding the incident and information about steps that you can take to help protect your information.

**What Happened?** Recently, we learned that some of your personal information may have been involved in a data security incident we experienced. The incident began on July 9, 2024, when we discovered suspicious activity that temporarily disrupted the operability of our computer network. We promptly took steps to secure the environment and began an investigation to determine the nature and scope of the issue. We also began working to restore impacted systems as quickly as possible, and engaged digital forensic specialists to conduct an investigation into what happened and whether personal information was accessed or acquired without authorization. The investigation determined that some data may have been acquired between July 8, 2024 and July 9, 2024. We then completed a comprehensive and thorough review of the data potentially involved to identify what personal information was impacted and to whom it belonged. We advised the applicable health benefit plan and/or the health plan’s third party administrator that information regarding some of their plan participants was affected. We then coordinated with <<b2b\_text\_2 (Client)>> to issue this notification to you.

Please note that we have no evidence of fraudulent misuse, or attempted misuse, of the potentially impacted information.

**What Information was Involved?** The information that may have been affected in connection with this incident includes your name as well as <<b2b\_text\_3 (Data Elements)>><<b2b\_text\_4 (Data Elements cont.)>>.

**What Are We Doing?** As soon as we discovered the incident, we took the steps discussed above. In addition, we reported the incident to law enforcement. To reduce the likelihood of a similar incident occurring in the future, we implemented additional measures to enhance the security of the network environment.

We are also providing you with access to <<Monitoring Term Length (Months)>> months of credit monitoring and fully managed identity theft recovery services through Kroll. You have until <<b2b\_text\_6 (activation deadline)>> to activate the services offered at no charge to you.

**What You Can Do.** You can follow the recommendations included with this letter to protect your personal information. We recommend that you review current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

You can also activate the complementary services offered to you through Kroll by following the instructions below.

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](http://info.krollmonitoring.com).

Additional information describing your services is included with this letter.

**For More Information:** If you have questions about this letter or need assistance, please do not hesitate to reach out to our designated call center at Kroll at 1-866-408-2595 Monday through Friday from 9:00 am to 6:30 pm Eastern Time, excluding holidays and they will be happy to provide you with additional information.

We take your trust in us and this matter very seriously. The security and privacy of patient data is among our highest priorities. Please accept our apologies for any concern or inconvenience this may cause you.

Sincerely,

The Phia Group, LLC

PO Box 313

Canton, MA 02021

## Steps You Can Take to Help Protect Your Personal 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 (the "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 [www.annualcreditreport.com/](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](http://www.equifax.com)

### **Experian**

P.O. Box 9532  
Allen, TX 75013  
1-888-397-3742  
[www.experian.com](http://www.experian.com)

### **TransUnion**

P.O. Box 2000  
Chester, PA 19016  
1-833-799-5355  
[www.transunion.com/  
get-credit-report](http://www.transunion.com/get-credit-report)

**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 [www.annualcreditreport.com](http://www.annualcreditreport.com). For TransUnion: [www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts).

**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. For TransUnion: [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze).

**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](http://consumer.ftc.gov)  
877-438-4338

### **Maryland Attorney General**

200 St. Paul Place  
Baltimore, MD 21202  
[www.marylandattorneygeneral.gov/  
Pages/CPD](http://www.marylandattorneygeneral.gov/Pages/CPD)  
888-743-0023

### **Oregon Attorney General**

1162 Court St., NE  
Salem, OR 97301  
[www.doj.state.or.us/  
consumer-protection](http://www.doj.state.or.us/consumer-protection)  
877-877-9392

### **California Attorney General**

1300 I Street  
Sacramento, CA 95814  
[www.oag.ca.gov/privacy](http://www.oag.ca.gov/privacy)  
800-952-5225

### **New York Attorney General**

The Capitol  
Albany, NY 12224  
800-771-7755  
[ag.ny.gov](http://ag.ny.gov)

### **Rhode Island Attorney General**

150 South Main Street  
Providence, RI 02903  
[www.riag.ri.gov](http://www.riag.ri.gov)  
401-274-4400

### **Iowa Attorney General**

1305 E. Walnut Street  
Des Moines, Iowa 50319  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)  
888-777-4590

### **NY Bureau of Internet and Technology**

28 Liberty Street  
New York, NY 10005  
[www.dos.ny.gov/consumerprotection/](http://www.dos.ny.gov/consumerprotection/)  
212.416.8433

### **Washington D.C. Attorney General**

400 S 6th Street, NW  
Washington, DC 20001  
[oag.dc.gov/consumer-protection](http://oag.dc.gov/consumer-protection)  
202-442-9828

**Kentucky Attorney General**  
700 Capitol Avenue, Suite 118  
Frankfort, Kentucky 40601  
[www.ag.ky.gov](http://www.ag.ky.gov)  
502-696-5300

**NC Attorney General**  
9001 Mail Service Center  
Raleigh, NC 27699  
[ncdoj.gov/protectingconsumers/](http://ncdoj.gov/protectingconsumers/)  
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 [www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf)

## KROLL

### TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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 will 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 in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.