

December 20, 2023

VIA EMAIL

Maryland Office of the Attorney General
Attn: Security Breach Notification
Idtheft@oag.state.md.us

RE: Notification of Security Breach

On November 30, 2023, Chimerix, Inc.'s former payroll company, Paycor, notified us that they were informed of a cyber vulnerability in software utilized by Paycor (Progress Software's MOVEit Transfer software). An unauthorized third party exploited this cyber vulnerability in May 2023 and obtained certain files and information transferred through the software. Paycor, with the assistance of an outside forensic data analysis company (Charles River Associates), has determined that some of Chimerix employees' sensitive information was affected as a result of this incident. By way of background, Paycor took over from Fidelity and was our payroll vendor from March 1, 2022 through November 30, 2022.

The Company has 1 employee in Maryland whose data was compromised. This employee is being notified of the breach using the attached sample notice, which will be sent by email and mail to the affected employee. Additionally, we sent the affected employee two articles from our Employee Assistance Program which offer advice on how they can protect themselves from identity theft and resource information in the event something occurs.

The Company last used Paycor as its payroll provider in 2022, and no longer uses Paycor to administer payroll.

If you have any questions or require additional information, please contact Barbara Berg, Executive Director, Human Resources at 919.313.2969.

Sincerely,

CHIMERIX, INC.



Barbara Berg
Executive Director, Human Resources

December 20, 2023

Employee Name
Employee Address
Employee City, MD and Zip Code

NOTICE OF DATA BREACH

Dear Employee Name:

We respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information.

WHAT HAPPENED?

On November 30, 2023, our former payroll company, Paycor, notified us that they were informed of a cyber vulnerability in software utilized by Paycor (Progress Software's MOVEit Transfer software). An unauthorized third party exploited this cyber vulnerability in May 2023 and obtained certain files and information transferred through the software. Paycor, with the assistance of an outside forensic data analysis company (Charles River Associates), has determined that some of our employees' sensitive information was affected as a result of this incident. You may recall that Paycor took over from Fidelity and was our payroll vendor from March 1, 2022 through November 30, 2022.

Paycor will not be providing individual notice to you. They have notified law enforcement of the breach.

WHAT INFORMATION WAS INVOLVED?

The data accessed included personal information such as:

- **Name.**
- **Birth date.**
- **Social Security Number.**

To our knowledge, the data accessed did not include:

- **Medical or health insurance information.**
- **Credit card number.**
- **Bank account number.**



CHIMERIX

WHAT WE ARE DOING

Chimerix values your privacy and deeply regrets that this incident occurred. Chimerix is no longer using Paycor as its payroll company and has not used Paycor since 2022. Chimerix is using a different payroll company to prevent a recurrence of such an attack and to protect the privacy of its valued employees.

Chimerix will work with law enforcement to ensure the incident is properly addressed.

WHAT YOU CAN DO

Please also review the attachment to this letter, "Steps You Can Take to Further Protect Your Information," for further information on steps you can take to protect your information.

Additionally, included with this letter are two articles from our Employee Assistance Program which offer advice on how to protect yourself from identity theft and resource information in the event something occurs.

FOR MORE INFORMATION

For further information and assistance, please contact me at 919-313-2969.

Sincerely,

CHIMERIX, INC.

Barbara Berg
Executive Director of Human Resources

Steps You Can Take to Further 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. Be on the lookout for warning signs that your information is being misused. Such signs include:

- Receiving credit cards for which you did not apply;
- Being denied credit or offered credit at less favorable terms for no apparent reason;
- Receiving calls or letters from debt collectors or businesses about merchandise or services you did not buy; and
- Missing bills and other pieces of mail.

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, including your state attorney general and the Federal Trade Commission (FTC).

To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

- **Obtain and Monitor Your Credit Report**

We recommend that you 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, calling toll-free 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 can access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action> or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 2002
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
P.O. Box 1000
Chester, PA 19016

- **Consider Placing a Fraud Alert on Your Credit Report**

We recommend placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. 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.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://consumer.ftc.gov/identity-theft-and-online-security>.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Be aware that if there are unauthorized charges on your credit report, you may be the victim of identity theft.

OTHER IMPORTANT INFORMATION

- **Security Freeze**

You have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency listed below. 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.

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

1-800-349-9960

<https://www.equifax.com/personal/credit-report-services/>

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

1-888-397-3742

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

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

1-888-909-8872

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

STATE SPECIFIC CONTACT INFORMATION

- **Maryland** residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at <https://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>, or by sending an email to idtheft@oag.state.md.us, or calling 410-576-6491.