



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

August 30, 2024

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

By Email

To Whom It May Concern:

I am writing on behalf of Octapharma Plasma, Inc. ("the Company") to notify you that the Company recently determined that a data security incident impacted personal information on its network. This included the information of Maryland residents.

On April 17, 2024, the Company detected suspicious activity on its IT systems. Upon detection, the Company promptly triggered its incident response processes, including launching an investigation with the assistance of third-party cybersecurity experts and the FBI. The investigation identified evidence that, on April 17, 2024, an unauthorized party had acquired data stored in the Company's file share systems. Based on the comprehensive data analysis that was performed and ultimately completed on August 2, 2024, it appears that the impacted data included the personal information of Maryland residents.

Approximately 5,230 Maryland residents have been identified as potentially impacted. The potentially impacted information varied by individual and may have included: name, Social Security number, passport number, driver's license number, student ID number, financial account number, and health information or donor eligibility information.

Upon learning that the Company's systems were accessed by an unauthorized party, the Company promptly took steps to secure the systems and contain the incident. The Company also launched an investigation with the support of third-party cybersecurity experts and notified law enforcement regarding the incident. To reduce the risk of similar events happening in the future, the Company is working to further enhance its security controls, including by undertaking a review of its technical security safeguards.

The Company plans to provide notice by mail to affected Maryland residents, which includes information regarding credit reporting agencies, government resources, security freezes, fraud alerts, and other identity protection tools. A sample copy of such notice is attached. The Company is also offering credit monitoring and identity protection services for two years through IDX, at no cost to the impacted individuals.

Please feel free to contact me at the information below if you have any questions or require additional information.

Sincerely,

/s/ Paul Otto

Paul Otto
(202) 637-5887
paul.otto@hoganlovells.com



P.O. Box 989728
West Sacramento, CA 95798-9728

<<First Name>> <<Middle Name>> <<Last Name>> <<Suffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

Enrollment Code: <<ENROLLMENT>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 30, 2024

NOTICE OF DATA BREACH

Dear <<First Name>> <<Middle Name>> <<Last Name>>,

I am writing on behalf of Octapharma Plasma, Inc. ("Octapharma" or "the Company") to notify you that we recently determined a data security incident impacted personal information on our network. Some of your personal information may have been impacted in this incident. We are providing this letter to help you understand what happened and what we are doing in response. We are taking this matter seriously and remain committed to protecting your information.

What Happened? On April 17, 2024, Octapharma detected suspicious activity on its IT systems. We took prompt action to respond to this incident, including launching an investigation with the assistance of third-party cybersecurity experts and the FBI. We determined that we were the victim of a data security incident by an unauthorized party. The incident has been contained and the investigation has concluded. The investigation identified evidence that, on April 17, 2024, an unauthorized party acquired information stored in the Company's file share systems. Based on the comprehensive data analysis that was performed and ultimately completed on August 2, 2024, we were able to determine what information was affected and to whom the information related. As a result of this review, it appears that some of your personal information may have been impacted.

What Information Was Involved? The potentially impacted information varied by individual and may have included your: <<Variable Text 1>>.

What We Are Doing. Upon learning that Octapharma systems were accessed by an unauthorized party, we promptly took steps to secure the systems and contain the incident. We also launched an investigation with the support of third-party cybersecurity experts and the FBI. To reduce the risk of similar events happening in the future, Octapharma is working to further strengthen its security controls, including by undertaking a review of our technical security safeguards. We also have arranged for you to obtain, at no cost to you, 24 months of credit monitoring services from IDX, a provider of identity theft protection. Information regarding these services is included below.

What You Can Do. We encourage you to sign up for the free credit monitoring and other services from IDX. These services can help you stay alert to and protected against potential misuses of your information. You can enroll by calling 1-877-211-5399, scanning the QR code above, or visiting <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9:00am–9:00pm EST. Please note the deadline to enroll is December 2, 2024. We also recommend that you remain vigilant by reviewing your account statements and monitoring your free credit reports for signs of suspicious activity. Please find additional information in Attachment 1 to this letter.

For More Information. We value transparency, and we have set up a dedicated call center to provide additional information regarding this incident. If you have questions or concerns regarding this incident, please call 1-877-211-5399 toll-free, Monday through Friday 9:00am–9:00pm EST (excluding holidays).

Sincerely,

Octapharma Plasma, Inc.

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Whether or not you enroll in the credit monitoring product offered, you also have the right to place an initial fraud alert on your file at no cost. An initial fraud alert lasts one (1) year and is placed on a consumer's credit file. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Fraud alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A fraud alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies. You may also contact any of the consumer reporting agencies or the FTC for more information regarding fraud alerts. The contact information for the three nationwide credit reporting agencies is:

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian

P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
<https://www.experian.com/help/>

TransUnion

P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
<https://www.transunion.com/credit-help>

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. We encourage you to review your rights pursuant to the FCRA by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcement for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself and prevent such activity. If you are a resident of the District of Columbia, Iowa, Maryland, New York, North Carolina, or Oregon, you can also reach out to your respective state's Attorney General's office at the

contact information below. Residents of all other states can find information on how to contact your state attorney general at <https://www.naag.org/find-my-ag/>.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357)
www.ftc.gov/idtheft

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, DC 20001
1-202-727-3400
oag.dc.gov

Oregon Department of Justice
1162 Court Street NE
Salem, OR 97301
1-877-877-9392
<https://justice.oregon.gov>

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023
www.marylandattorneygeneral.gov

New York Attorney General's Office
The Capitol
Albany, NY 12224-0341
1-800-771-7755
<https://ag.ny.gov/consumer-frauds-bureau/identity-theft>

**Consumer Protection Division
Office of the Attorney General of Iowa**
1305 E. Walnut Street
Des Moines, IA 50319
1-515-281-5926
www.iowaattorneygeneral.gov

North Carolina Department of Justice
114 West Edenton Street
Raleigh, NC 27603
1-919-716-6400
<https://ncdoj.gov/protecting-consumers/identity-theft/>

Security Freeze Information

You have the right to request a free security freeze (aka "credit freeze") on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a credit freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A credit freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. You may also contact any of the consumer reporting agencies or the FTC for more information regarding security freezes.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
<http://www.equifax.com/personal/credit-report-services/credit-freeze/>
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
<https://www.transunion.com/credit-freeze>
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.