ALEXION
AstraZeneca Rare Disease

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

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

Notice of Data Breach

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

Alexion Pharmaceuticals, Inc. (Alexion) takes the protection of your personal data seriously. Today, we are reaching out to make you aware of an incident that involved some of your personal information. Please read this notice carefully, as it provides information about the incident, the personal data involved, the steps we have taken to ensure the security of the data, and the resources available to you to help protect yourself against any potential unauthorized use of your personal data. We have included our contact details below should you need any further information.

What Happened?

On February 8, 2024, an unauthorized third party accessed the database of a vendor we use to support our Risk Evaluation and Mitigation Strategy (REMS) program. The breached vendor, Cisiv Ltd., was a subcontractor to our REMS vendor, PPD, and provides the database and REMS platform used to manage and collect data from the REMS surveys.

When Cisiv discovered the incident on February 12, 2024, they immediately took steps to contain the intrusion and contained it the same day. Cisiv also engaged a leading cyber security forensics consultant to investigate the incident. During the subsequent investigation, it was determined that certain personal data was acquired by that unauthorized third party, and on April 16, 2024, we learned that your personal data was impacted.

What Information Was Involved?

As part of the REMS, we periodically send surveys required by the Food and Drug Administration (FDA) to assess the effectiveness of the REMS program in communicating important information about the risks and safe use of our products. You are receiving this notice because the vendor determined that your name, address, email address, phone number, and the fact that you took a survey related to one of our products was acquired by the third party.

What We Are Doing

We take your privacy seriously, and we endeavor to protect all your personal data. To do so, we will continue to review, audit, and improve our security controls and processes and those of our vendors. As noted, upon learning of the incident, an investigation was conducted to determine the details and scope of the incident and what personal data was impacted. Cisiv hired a third-party cybersecurity forensics consultant to ensure the security of its systems and the vendor put in place additional security controls to protect data.

We have **no** indication that any of your information has been used to commit fraud or identity theft. However, as a precaution and to help alleviate concerns, we are offering you complimentary identity monitoring for one year from Kroll. Your identity monitoring services through Kroll include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

- 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. Additional information describing your services is included with this letter.

What You Can Do

Supplemental information is attached to this letter, including the Steps You Can Take to Protect Your Data as guidance on further protecting your personal data. We encourage you to remain vigilant for incidents of fraud and identity theft by carefully reviewing your payment card or personal account statements for unauthorized charges and monitoring free credit reports for fraudulent activity or errors resulting from the incident.

If you suspect an unauthorized charge has been placed on your account, we encourage you to report it to your payment card issuer. According to the payment card brands' policies, you are not responsible for unauthorized charges to your account if you report them in a timely manner.

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

For More Information

If you have additional questions, please call (866) 528-6281, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Arshad Mujeebuddin, Vice President, Patient Safety
Laura Marchant, Global Data Protection Officer
Alexion Pharmaceuticals, Inc.
121 Seaport Boulevard
Boston, MA 02210 USA

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

STEPS YOU CAN TAKE TO PROTECT YOUR DATA

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission, local law enforcement, and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. You should obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information follows for the Federal Trade Commission, as well certain state Attorney General Offices that we are required to provide pursuant to state law.

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

For DC residents: *District of Columbia Office of the Attorney General*, 400 6th Street NW, Washington, DC 200001, 202-727-3400, https://oag.dc.gov/

For Maryland residents: *Maryland Office of the Attorney General*, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us

For New York residents: *New York State Attorney General,* The Capitol Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov/

New York State Police, 1220 Washington Ave, Bldg. 22, Albany NY, 12226, 1-866-SAFENYS, 1-888-NYCSAFE, https://www.ny.gov/

New York Department of State's Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave, Albany, NY 12231-0001, 1 (800) 697-1220, https://troopers.ny.gov/contact-us

For North Carolina residents: *North Carolina Office of the Attorney General*, 9001 Mail Service Center, Raleigh, NC 27699-9001, 877-566-7266, www.ncdoj.gov

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—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 one year. 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.

To place a fraud alert on your credit reports, please contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If a creditor can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, please contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You will need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save time by lifting the freeze only at that particular credit bureau. Otherwise, you will need to make the request with all three credit bureaus.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.