

Reed Abrahamson
Partner
reed.abrahamson@faegredrinker.com
+1 202 230 5672 direct

Faegre Drinker Biddle & Reath LLP
1500 K Street, NW, Suite 1100
Washington, DC 20005
+1 202 230 5000 main
+1 202 842 8465 fax

August 23, 2023

Via Email to Idtheft@oag.state.md.us

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

Re: Notice of Data Incident

Dear Attorney General Brown,

I am writing on behalf of Amgen Inc. to inform you of a recent incident that may have affected the personal information of five (5) Maryland state residents.

On June 30, 2023, Amgen received reports from certain users of the Embark Application, an app designed to support patients taking ENBREL as a medication, that their user profiles displayed incorrect personal information. Amgen conducted a thorough investigation of the incident. That investigation revealed that, on and after June 3, 2023, through and including July 31, 2023, certain patients' personal information may have been inadvertently disclosed to a number of other users of the Embark Application due to a coding error by the vendor responsible for managing the Embark Application during data migration.

Based on our review, the potentially exposed information included names, mailing addresses, email addresses, dates of birth, medication information, and health insurance identification numbers. We have no evidence to date that the personal information has been misused and have confirmed with reasonable certainty that this incident did not compromise or disclose to other patients the affected individuals' account log-in credentials for the Embark Application.

After discovering the incident, the Amgen vendor successfully implemented an update to the Embark Application on July 31, 2023, safeguarding future personal information from being accessible to other patients. Although no personal financial information or social security information was involved, out of an abundance of caution, Amgen is also offering credit and identity theft resolution services at no cost to affected individuals for twenty-four (24) months.

We are in the process of providing notice to these individuals. Individual notifications detailing the incident and enrollment process will be mailed to affected individuals beginning on August 24, 2023. A template copy of the notification letter is enclosed.

Please contact me if you have any further questions about this incident.

Respectfully submitted,

Reed Abrahamson

Enclosure: Template copy of notification letter



Amgen Inc.
Thousand Oaks, CA 91320
www.amgen.com

<<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 Incident

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

Amgen Inc. (Amgen) writes to inform you that your personal information may have recently been inadvertently disclosed to other users of the Embark Application. This letter provides you with information about the nature of the incident and affected data and the immediate and additional corrective measures Amgen has taken to guard against future unauthorized disclosure of your personal data.

What Happened?

On June 30, 2023, Amgen received reports from certain users of the Embark Application that their user profiles displayed incorrect personal information. Amgen conducted a thorough investigation of the incident. That investigation revealed that, on and after June 3, 2023, through and including July 31, 2023, certain patients' personal information may have been inadvertently disclosed to a number of other users of the Embark Application due to a coding error by the vendor responsible for managing the Embark Application during data migration.

What Information Was Involved?

The potentially exposed information may have included your name, mailing address, email address, date of birth, medication information, and health insurance identification number.

What We Are Doing

We take the security of your personal information seriously. Therefore, after discovering the incident, the Amgen vendor successfully implemented an update to the Embark Application on July 31, 2023, to safeguard your personal information from being accessible to other patients.

Because this incident did not involve potential criminal activities, there is no ongoing law enforcement investigation. As such, this notice was not delayed as a result of a law enforcement investigation.

We have no evidence to date that your personal information has been misused and have confirmed with reasonable certainty that this incident did not compromise or disclose to other patients your account log-in credentials for the Embark Application. Out of an abundance of caution, we are making available to you 24 months of identity monitoring through Kroll, at no cost to you. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

What You Can Do

If you have not already done so, you can activate your identity monitoring services by following the instructions in the section below titled *Activating Your Complimentary Identity Monitoring*. Please continue to be vigilant about the security of your personal accounts and monitor them for unauthorized activity. Please report any suspicious activity to appropriate law enforcement or your state Attorney General.

Additionally, we recommend contacting your healthcare providers if bills don't arrive on time in case an identity thief has changed the billing address, check the Explanation of Benefits forms from their insurance company for irregularities, and review your medical records for errors. If you spot anything unusual, contact their insurance company about possible medical identity theft or ask for a new account number.

Activating Your Complimentary Identity Monitoring

To help protect your identity, we are offering you complimentary access to Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration for 24 months.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> 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.

Again, we take your privacy seriously and regret any concern or inconvenience this incident may cause you. If you have additional questions, please contact us at:

Amgen Inc.
Privacy Compliance
One Amgen Center Drive
Thousand Oaks, CA 91320
(805) 313-5151 Local
(800) 867-6677 Toll-Free
privacy@amgen.com

Sincerely,

Amgen Privacy Compliance

Preventing Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Immediately report any suspicious activity to your bank or credit union. If you do find suspicious activity on your credit reports or other statements, call your local police or sheriff's office, or state Attorney General and file a report of identity theft. You have a right to a copy of the police report, and you may need to give copies of the police report to creditors to clear up your records and access some services free to identity theft victims.

Under the U.S. Fair Credit Reporting Act and other laws, you have certain rights that can help protect yourself from identity theft. Many of these are explained in this letter and at www.identitytheft.gov/#/Know-Your-Rights. For example, you are entitled to one free credit report annually from each of the three major credit reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. You may also contact the three major credit reporting agencies directly to request a free copy of your credit report.

In addition, at no charge, you can have these credit bureaus place a short-term or an extended "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because a fraud alert tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. Once one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. If you wish to place a fraud alert or have any questions regarding your credit report, please contact any one of the agencies listed below. Please note no one except you is allowed to place a fraud alert on your credit report.

General contact information for each agency:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016-2000
1-866-349-5191	888-397-3742	800-888-4213
www.equifax.com	www.experian.com	www.transunion.com

To add a fraud alert:

Equifax	(888) 202-4025, Option 6 or	https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
Experian	(714) 830-7000, Option 2 or	https://www.experian.com/fraud/center.html
TransUnion	(800) 916-8800, Option 0 or	https://www.transunion.com/fraud-alerts

You may also place a security freeze on your credit reports, free of charge. A security freeze, also known as a "credit freeze," prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. Unlike a fraud alert, you must place a security freeze separately on your credit file at each bureau. You can use the following addresses and contact information to place a security freeze with each major credit bureau:

Equifax Security Freeze. 1-888-298-0045. P.O. Box 1057881, Atlanta, GA 30348-0241.
www.equifax.com/personal/credit-report-services/credit-freeze;

Experian Security Freeze. 1-888-EXPERIAN or 1-888-397-3742. P.O. Box 9554, Allen, TX 75013.
www.experian.com/freeze/center.html; or

TransUnion. 1-800-680-7289. Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19016-2000.
www.transunion.com/credit-freeze

The Federal Trade Commission also provides additional information about credit freezes here:
<https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs>.

In order to request a security freeze, you may need to supply your full name (including middle initial, as well as Jr., Sr., II, III, etc.), date of birth, Social Security number, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or another statement to show proof of your current address. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning your identity theft.

The credit reporting agencies must place a security freeze on your credit report within one (1) business day after receiving a request by phone or secure electronic means and within (3) business days after receiving your request by mail. The credit bureaus must then send written confirmation to you within five (5) business days of placing the security freeze, along with information about how to remove or lift the security freeze in the future.

You can further educate yourself regarding identity theft, fraud alerts, freezes, and the steps you can take to protect yourself by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission encourages those who discover their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement or your state Attorney General.

The Federal Trade Commission can be reached at:

Federal Trade Commission
Consumer Resource Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.identitytheft.gov or www.ftc.gov

OTHER IMPORTANT INFORMATION

You may obtain information about avoiding identity theft from the relevant regulators of your state of residence, including:

California residents:

You can visit the California Attorney General's site (www.oag.ca.gov/idtheft) for information on protection against identity theft.

Kentucky residents:

Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118, Frankfort, Kentucky 40601; phone: 1-502-696-5300; www.ag.ky.gov

Maryland residents:

You may obtain information about avoiding identity theft at: Office of the State of Maryland Attorney General, 200 St. Paul Place Baltimore, MD 21202; phone: 1-888-743-0023; www.marylandattorneygeneral.gov.

New Mexico residents:

The Fair Credit Reporting Act (FCRA) provides certain rights in addition to the right to receive a copy of your credit report (including a free copy once every 12 months), including the right to ask for a credit score, dispute incomplete or inaccurate information, limit "prescreened" offers of credit and insurance, be told if information in your credit file has been used against you, and seek damages from violators. You may have additional rights under the FCRA not summarized here, and identity theft victims and active-duty military personnel have specific additional rights pursuant to the FCRA. You can review these rights by visiting www.consumerfinance.gov/f/201904_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York residents:

The Office of the Attorney General may be reached at The Capitol, Albany, NY 12224-0341; phone: 1-800-771-7755; ag.ny.gov

North Carolina residents:

You may obtain information about avoiding identity theft at: North Carolina Attorney General's Office 9001 Mail Service Center Raleigh, NC 27699-9001; phone: 919-716-6400; ncdoj.gov

Oregon residents:

You may obtain information about avoiding identity theft at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; phone: 1-877-877-9392; www.doj.state.or.us/.

Rhode Island residents:

You may obtain information about preventing and avoiding identity theft from Rhode Island's Attorney General Office: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903; phone: 401-274-4400; <http://www.riag.ri.gov>.

Washington D.C. residents:

You may obtain information about avoiding identity theft at: Office of the Attorney General for the District of Columbia, 441 4th Street, NW, Washington, DC 20001; phone: 202-727-3400; <https://oag.dc.gov/>.

Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).



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.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

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.