

Reed Abrahamson
Partner
Reed.Abrahamson@faegredrinker.com
202-230-5672 direct

Faegre Drinker Biddle & Reath LLP
1500 K Street, NW, Suite 1100
Washington, DC 20005
+1 202 842 8800 main
+1 202 842 8465 fax

September 25, 2024

VIA E-MAIL 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 Security Incident

Dear Attorney General Brown,

I am writing on behalf of Amgen Inc. ("Amgen") to inform you of a recent data security incident that may affect the personal information of Maryland state residents.

On or about September 29, 2023, Amgen service provider Sirva, Inc. ("Sirva") became aware of suspicious activity involving its network and began an investigation. The investigation determined certain Sirva systems were accessed by unknown actors between August 16, 2023 and October 17, 2023, and that during this time certain files were copied. Further, on March 21, 2024, Sirva's investigation revealed that some personal information relating to individuals associated with Sirva and certain Sirva clients had been accessed. On April 10, 2024, Sirva notified Amgen that some individuals affiliated with Amgen may have been impacted. Amgen promptly coordinated with its legal counsel and with Sirva to provide notifications regarding the incident to affected individuals and to regulators to the extent required by applicable law. Following that initial notification on April 10, 2024, Sirva provided Amgen with information on August 8, 2024 about additional impacted individuals. This notification is being made to you on the basis of that additional information from Sirva.

Based on information Amgen has received from Sirva, we are required to provide notice pursuant to Maryland law to 11 Maryland residents. Per details from Sirva, the impacted files pertaining to these individuals include: contact information, date of birth, social security number, employment information, and/or gender identification. Amgen is in the process of providing notice to these individuals as required by Maryland law. No Amgen systems were impacted by this incident.

A template copy of the notification letter sent to affected individuals is enclosed as Exhibit A. Please contact me if you have any further questions about this incident.

September 25, 2024

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Reed Abrahamson". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Reed Abrahamson

Partner

Enclosure: Template copy of notification letter to individuals

EXHIBIT A



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

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

NOTICE OF VENDOR DATA BREACH

Dear <<first_name>> <<last_name>>:

Amgen has learned that one of our service providers, Sirva Relocation, LLC, and its parent company, Sirva, Inc. (together, "Sirva"), experienced a data security incident that may have involved some of your personal information that Sirva received and processed on behalf of Amgen. Amgen takes the protection and proper use of your information very seriously; therefore, we are contacting you to explain the incident and measures taken to protect your information.

What Happened?

On or about September 29, 2023, Sirva became aware of suspicious activity involving its network and immediately began an investigation. The investigation determined that certain Sirva systems were accessed by unknown actors between August 16, 2023 and October 17, 2023, and that during this time certain files were copied. Sirva undertook a thorough and time-consuming review of the potentially involved data to identify its contents and to whom it relates. On August 8, 2024, Sirva informed Amgen that, based on its ongoing review of the involved data, some information related to you may have been impacted by the incident.

What Information Was Involved?

Your identifiable information that may have been accessed may include one or more of the following:

- Name
- Contact Information
- Non-U.S. Address
- Credit/Debit Card Information
- Date of Birth
- Employment Information, Including Salary
- Financial Accounts Information
- Gender Identification
- Medical/Health Information
- Passport Information
- Sirva File Number
- Social Security Number/Social Insurance Number
- Unique or Other Government-Issued ID Number
- Loan Information
- Taxpayer Identification Number

What We Are Doing

At Amgen, the confidentiality, privacy, and security of your information is a top priority, and we take this incident very seriously. Upon first receiving initial notice from Sirva, Amgen immediately commenced an investigation and worked with Sirva to better understand the nature and scope of the incident and any impact to the personal information of Amgen personnel. The investigation actions included steps to assess and secure the Sirva network, ongoing review of the relevant involved data, and notification to law enforcement and regulators, as applicable. The incident did not affect Amgen's own systems.

As part of our ongoing commitment to the security of your information, we have worked with Sirva to evaluate their policies and Sirva has implemented additional measures and safeguards to enhance the security of its network and protect against this type of incident in the future. We are also providing notification of this incident to global data protection authorities and applicable U.S. state regulators, including state Attorneys General, where legally required.

What You Can Do

To assist you in protecting your information, we have secured the services of Kroll to provide identity monitoring at no cost to you for <<Monitoring Term Length (Months)>> months, or longer for residents of certain U.S. states where required by applicable law. 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.

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 the identity monitoring services available to you is included with this letter.

We also encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring free credit reports for suspicious activity and to detect errors particularly over the next 12 to 24 months. Suspicious activity should be promptly reported to relevant parties, including an insurance company and/or financial institution.

Additional resources can be found below, and in the attached *Steps You Can Take to Help Protect Your Personal Information*.

More Information

We regret this incident occurred and any inconvenience or concern it has caused you.

- For more information about the services available to you via Kroll, or for assistance signing up for those services, please call Kroll at (866) 997-0255 between 8:00 am and 5:30 pm Central Time, Monday through Friday, excluding major U.S. holidays.
- For questions about the data security incident, please contact Amgen Human Resources. If you are presently employed at Amgen, you can submit an HR Request for information via the MyHR portal or call HR Connect at +1 805-447-1111 (U.S.) or +787-916-1111 (Puerto Rico). If you are not currently an Amgen employee, you can email HR Connect at hrconnect@amgen.com or call HR Connect at +1 805-447-1111 (U.S.) or +787-916-1111 (Puerto Rico).

Sincerely,

Amgen Inc.

One Amgen Center Drive, Thousand Oaks, CA 91320

Steps You Can Take to Help Protect Your Personal Information

Activate Identity Monitoring Services

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



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.

Monitor Your Accounts

If you are a U.S. individual, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. 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. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

- Full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- Addresses for the prior two to five years;
- Proof of current address, such as a current utility bill or telephone bill;
- A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
- A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should you wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298 0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect their personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For Massachusetts residents, individuals have the right to obtain a police report with respect to this incident.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and (401) 274-4400. Under Rhode Island law, individuals have the right to file or obtain any police report filed in regard to this event. There are approximately 189 Rhode Island residents that may be impacted by this event.