



<<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>> <<middle_name>> <<last_name>> <<suffix>>,

Amgen recently learned that one of our service providers experienced a data security incident that may have involved some of your personal information. 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 May 27, 2021, Amgen was notified by one of our service providers, ZS Associates (“ZS”), of a security incident in which an unauthorized party compromised a ZS service account and accessed and may have downloaded certain files related to Amgen between April 21, 2021 and May 14, 2021. ZS provides consulting and professional services to Amgen.

On May 17, 2021, ZS identified and disabled the compromised account and has been working with law enforcement and outside experts to investigate the security incident. This notice provides information about the ZS incident, our response, and resources available to affected patients.

What Information Was Involved?

Based on our review to date, these files included names; email addresses; city, state and zip code of residence; age; gender; and whether a person had commercial or government health insurance. Based on our investigation to date, we have determined that the impacted files also included information about marketing materials Amgen sent to you related to Repatha.

No identifiable health insurance information, Social Security numbers, or personal financial information such as credit card or bank account numbers were involved.

What We Are Doing

At Amgen, the confidentiality, privacy, and security of patient information is a top priority, and we take this incident very seriously. Upon receiving notice from ZS, Amgen immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Amgen patients and data. Additionally, we retained a third-party forensic firm to conduct a thorough investigation of the data and information. The incident did not affect Amgen’s own systems.

As part of our ongoing commitment to the security of your information, we are working with ZS to evaluate their policies and additional measures and safeguards to protect against this type of incident in the future. We are also providing the legally required notification of this incident to the applicable State Attorneys General.

Although no financial information or social security information was involved, out of an abundance of caution, we are providing you with complimentary credit and identity monitoring services.

What You Can Do

Although no social security or other personal financial or health insurance information was involved, 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. Please review the attachment called *Preventing Identity Theft and Fraud* for more information on ways to protect yourself against the potential misuse of your information.

Also, to assist you in monitoring your information, we are offering you one year of free credit and identity monitoring services through a company called Kroll.

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

*You have until **September 22, 2021** to activate your identity monitoring services.*

Membership Number: <<**Member ID**>>

Additional information describing your services is included with this letter.

For More Information

We regret this incident occurred and any inconvenience or concern it has caused you. Should you have any further questions or concerns regarding this matter, please call 1-855-731-3194 between 8:00am and 5:30pm Central time, Monday through Friday (excluding major U.S. national holidays), or visit www.amgen.com/dataincident.

To report an adverse event or product complaint that has occurred during the use of an Amgen product, call Amgen Medical Information at 800-77-AMGEN (800-772-6436).

Preventing Identity Theft and Fraud

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling tollfree 1-877-322-8228, 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 print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to obtain or purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact these national credit reporting agencies to request a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files. Contact information for these agencies is as follows:

Equifax
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Other Important State Information

If you are the victim of identity theft, you may also file a report with your local police or the police in the community where the identity theft took place and obtain a copy of that report.

For 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>.

For 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, 1-888-743-0023 www.marylandattorneygeneral.gov.

For 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, 202-727-3400 <https://oag.dc.gov/>

For 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, 919-716-6400 www.ncdoj.gov.

For New Mexico Residents:

The Fair Credit Reporting Act 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, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For California Residents:

You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Iowa Residents:

You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents:

You may request a free security freeze from the credit bureaus listed above. You may need to supply your full name, date of birth, Social Security number, all addresses for the past five years, email address, a copy of your state identification card or driver's license, and proof of your current address. If you are a victim of identity theft, include a copy of any police or investigative report, or complaint to a law enforcement agency. The credit reporting agencies must place a freeze on your credit report one business day after receiving your request by phone or secure electronic means, and three business days after receiving your request by mail. The credit bureaus must confirm the freeze within five business days and provide information about how to remove or lift the freeze.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico and Vermont 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.



<<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>> <<middle_name>> <<last_name>> <<suffix>>,

Amgen recently learned that one of our service providers experienced a data security incident that may have involved some of your personal information. 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 May 27, 2021, Amgen was notified by one of our service providers, ZS Associates (“ZS”), of a security incident in which an unauthorized party compromised a ZS service account and accessed and may have downloaded certain files related to Amgen between April 21, 2021 and May 14, 2021. ZS provides consulting and professional services to Amgen.

On May 17, 2021, ZS identified and disabled the compromised account and has been working with law enforcement and outside experts to investigate the security incident. This notice provides information about the ZS incident, our response, and resources available to affected patients.

What Information Was Involved?

Based on our review to date, these files included first names and email addresses. Based on our investigation to date, we have determined that the impacted files also included information about marketing materials Amgen sent to you related to Aimovig.

No identifiable health insurance information, Social Security numbers, or personal financial information such as credit card or bank account numbers were involved.

What We Are Doing

At Amgen, the confidentiality, privacy, and security of patient information is a top priority, and we take this incident very seriously. Upon receiving notice from ZS, Amgen immediately commenced an investigation to better understand the nature and scope of the incident and any impact on Amgen patients and data. Additionally, we retained a third-party forensic firm to conduct a thorough investigation of the data and information. The incident did not affect Amgen’s own systems.

As part of our ongoing commitment to the security of your information, we are working with ZS to evaluate their policies and additional measures and safeguards to protect against this type of incident in the future. We are also providing the legally required notification of this incident to the applicable State Attorneys General.

Although no financial information or social security information was involved, out of an abundance of caution, we are providing you with complimentary credit and identity monitoring services.

What You Can Do

Although no social security or other personal financial or health insurance information was involved, 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. Please review the attachment called *Preventing Identity Theft and Fraud* for more information on ways to protect yourself against the potential misuse of your information.

Also, to assist you in monitoring your information, we are offering you one year of free credit and identity monitoring services through a company called Kroll.

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

*You have until **September 22, 2021** to activate your identity monitoring services.*

Membership Number: <<**Member ID**>>

Additional information describing your services is included with this letter.

For More Information

We regret this incident occurred and any inconvenience or concern it has caused you. Should you have any further questions or concerns regarding this matter, please call 1-855-731-3194 between 8:00am and 5:30pm Central Time, Monday through Friday (excluding major U.S. national holidays), or visit www.amgen.com/dataincident.

To report an adverse event or product complaint that has occurred during the use of an Amgen product, call Amgen Medical Information at 800-77-AMGEN (800-772-6436).

Preventing Identity Theft and Fraud

As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely. 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 should also promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities, including the police and your state's attorney general, as well as the Federal Trade Commission ("FTC").

You may wish to review the tips provided by the FTC on fraud alerts, security/credit freezes and steps to you can take to avoid identity theft. For more information and to contact the FTC, please visit www.ftc.gov/idtheft or call 1-877-ID-THEFT (1-877-438-4338). You may also contact the FTC at: Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Credit Reports: You may obtain a free copy of your credit report once every 12 months from each of the three national credit reporting agencies by visiting <http://www.annualcreditreport.com>, by calling tollfree 1-877-322-8228, 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 print a copy of the request form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

Alternatively, you may elect to obtain or purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact these national credit reporting agencies to request a copy of your credit report or for general inquiries, including obtaining information about fraud alerts and placing a security freeze on your credit files. Contact information for these agencies is as follows:

Equifax
1-888-298-0045
www.equifax.com
P.O. Box 105788
Atlanta, GA 30348

Experian
1-888-397-3742
www.experian.com
P.O. Box 9554
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 2000
Chester, PA 19016

Fraud Alerts: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. Additional information is available at <http://www.annualcreditreport.com>.

Credit and Security Freezes: You may have the right to place a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies using the contact information above.

Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by requesting information in writing from the Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. NW, Washington, DC 20580.

Other Important State Information

If you are the victim of identity theft, you may also file a report with your local police or the police in the community where the identity theft took place and obtain a copy of that report.

For 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>.

For 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, 1-888-743-0023 www.marylandattorneygeneral.gov.

For 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, 202-727-3400 <https://oag.dc.gov/>

For 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, 919-716-6400 www.ncdoj.gov.

For New Mexico Residents:

The Fair Credit Reporting Act 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, and seek damages from violators. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For California Residents:

You can visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

For Iowa Residents:

You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts Residents:

You may request a free security freeze from the credit bureaus listed above. You may need to supply your full name, date of birth, Social Security number, all addresses for the past five years, email address, a copy of your state identification card or driver's license, and proof of your current address. If you are a victim of identity theft, include a copy of any police or investigative report, or complaint to a law enforcement agency. The credit reporting agencies must place a freeze on your credit report one business day after receiving your request by phone or secure electronic means, and three business days after receiving your request by mail. The credit bureaus must confirm the freeze within five business days and provide information about how to remove or lift the freeze.

For Colorado, Georgia, Maine, Maryland, New Jersey, Puerto Rico and Vermont 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.