

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Caleb W. Skeath

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5119
cskeath@cov.com

By Electronic Mail

September 8, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

**Re: Legal Notice of Information Security Breach Pursuant to
Md. Code Ann., Com. Law § 14-3501(h)(1)**

To Whom it May Concern:

In accordance with the above-referenced provision of Maryland law, I write to inform you of an information security breach affecting residents of Maryland.

On August 8, 2023, Freeport-McMoRan Inc. ("Freeport") identified suspicious activity on its systems and immediately launched an investigation. Freeport's investigation subsequently identified unauthorized activity within its information technology environment between approximately August 8 and August 11, 2023. On August 11, 2023, Freeport identified that an unauthorized third party had obtained personal information regarding certain individuals, including current and former Freeport employees.

Based on Freeport's investigation to date, the information that was obtained by the unauthorized third party included individuals' names, Social Security numbers, dates of birth, and email addresses.

Upon learning of this incident, Freeport took immediate steps to launch a comprehensive investigation, and has notified and been working with law enforcement. Freeport also retained third-party cybersecurity experts to investigate the incident and aid in securely bringing systems back online. Once it confirmed that an unauthorized third party had obtained personal information, Freeport quickly began working to identify and notify the individuals affected. To date, Freeport has not identified any indications of identity theft or fraud in connection with this incident.

Freeport intends to notify 3 potentially affected individuals who are residents of Maryland. Enclosed is a copy of the notification letter that Freeport will send to affected individuals via first-class mail on September 8, 2023. Freeport's assessment of the incident is ongoing, and Freeport will notify any additional affected residents of Maryland consistent with applicable law as they are identified.

COVINGTON

September 8, 2023

Page 2

The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by Freeport to protect personal information from further unauthorized access; (3) Freeport's address and a toll-free phone number to call for further information and assistance; (4) information on how the individual may enroll in free credit monitoring and other complimentary services arranged by Freeport; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free number, address, and website for the Federal Trade Commission and the Office of the Attorney General of Maryland, and a statement that individuals can obtain information on identity theft from these sources; and (8) advice that directs the individual to remain vigilant by reviewing account(s) for unusual activity and monitoring free credit reports.

If you have any questions or need further information regarding this incident, please contact the undersigned at cskeath@cov.com or (202) 662-5119.

Respectfully submitted,

/s

Caleb W. Skeath
Counsel for Freeport-
McMoRan Inc.

Enclosure

Freeport Minerals Corporation
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



Phoenix Corporate Office
333 N. Central Ave.
Phoenix, AZ 85004



September 8, 2023

NOTICE OF DATA BREACH

Freeport-McMoRan Inc. ("Freeport") recently announced it experienced a cybersecurity incident that impacted its information systems. You are receiving this letter because we have identified that some of your personal information was disclosed as part of this incident.

What Happened?

On August 8, 2023, we identified suspicious activity on our systems and immediately launched an investigation. Our investigation subsequently identified unauthorized activity within our information technology environment between approximately August 8 and August 11, 2023. On August 11, 2023, we identified that an unauthorized third party had obtained personal information regarding certain individuals, including current and former Freeport employees.

What Information was Involved?

Based on our investigation to date, the information that was obtained by the unauthorized third party included your name, date of birth, Social Security number, and email address.

What We are Doing.

We are offering free identity theft protection services through TransUnion for a period of 24 months. You may sign up for this service by following the instructions included in Attachment A.

When learning about this incident, we took immediate steps to launch a comprehensive investigation, and have notified and been working with law enforcement. We also retained third-party cybersecurity experts to investigate the incident and aid us in securely bringing our systems back online.

When we confirmed that an unauthorized third party had obtained personal information, we quickly began working to identify and notify the individuals affected. Our priority has been the safety, protection and well-being of our employees.

What You Can Do.

Whether or not you elect to enroll in the identity theft protection services, we strongly recommend that you remain vigilant and regularly review and monitor all your credit history to guard against any unauthorized transactions or activity. We also recommend you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity. Attachment B contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information.

Please be assured that we are taking steps to address the incident and to protect the security of your data. If you have any questions about this notice or the incident, please call the Cyberscout help line at 1-888-499-1088 and give the fraud specialist your unique code listed in Attachment A. Representatives are available between 8 a.m. and 8 p.m. Eastern time, Monday through Friday, excluding holidays.

000010102G0500

P

ATTACHMENT A

Identity Theft Protection Services

What Do the Services Entail?

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or if you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How Do I Enroll for the Free Services?

To enroll in Credit Monitoring services at no charge, log on to **<https://secure.identityforce.com/benefit/freeport>** and follow the instructions provided. When prompted please provide the following unique code to receive services:

[REDACTED]

For you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What If I Have Questions Regarding This Incident and the Identity Threat Protection Services?

Representatives are available for 90 days from the date of this letter to assist you with questions regarding this incident between 8 a.m. and 8 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-888-499-1088 and give the fraud specialist with your unique code listed above.

ATTACHMENT B

Additional Information

To protect against possible fraud, identity theft or other financial loss, we encourage you to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you should consider contacting your local law enforcement agency, your State's attorney general or the Federal Trade Commission.



INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit **www.annualcreditreport.com** or call toll-free 1-877-322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three credit reporting agencies below:

Equifax:

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

Experian:

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

TransUnion:

Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major credit reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major credit reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days but can be renewed.

Credit Freeze: A credit freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one – including you – can open a new account. As a result, please be aware 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.

Placing a credit freeze is free. To place a credit freeze, contact all three credit reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, a copy of either a police report, investigative report or complaint to a law enforcement agency concerning identity theft

When you place a credit freeze, you will be provided a PIN to temporarily lift or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three credit reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charge monthly fees.

You also may contact the U.S. Federal Trade Commission (“FTC”) for further information on fraud alerts, credit freezes, credit locks and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024, by telephone at 1-877-382-4357 or online at www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General or the FTC.

District of Columbia Residents: The Attorney General can be contacted at the Office of the Attorney General, 400 6th Street NW, Washington, DC 20001; 1-202-727-3400; or <https://oag.dc.gov/>.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or <https://www.marylandattorneygeneral.gov/>.

New York Residents: The Attorney General can be contacted at 1-800-771-7755 or <https://ag.ny.gov/>. The Department of State Division of Consumer Protection can be contacted at 1-800-697-1220 or <https://dos.ny.gov/>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; or <http://www.ncdoj.gov>.

Rhode Island Residents: The Attorney General can be contacted at 1-401-274-4400 or <http://www.riag.ri.gov/>. You also may file a police report by contacting local or state law enforcement agencies.