NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
1550 Lamar Street, Suite 2000
Houston, Texas 77010-4106
United States of America

Direct line +1 713 651 5684
will.daugherty@nortonrosefulbright.com

Tel +1 713 651 5151
Fax +1 713 651 5246

July 30, 2024

Via email: idtheft@oag.state.md.us

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

Re: Notice of Security Incident

Dear Sir or Madam:

I am writing on behalf of my client, Gold Reserve Inc. ("Gold Reserve"), to notify your office of a cybersecurity incident.

On April 22, 2024, Gold Reserve discovered that an unauthorized third party gained access to a portion of its IT infrastructure ("Incident"). Gold Reserve immediately deployed countermeasures to secure its network and data from further unauthorized access and engaged third party cybersecurity experts to assist with containment, remediation, and conducting a forensic investigation to determine the nature and extent of the Incident. The forensic investigation determined that on the same day, the unauthorized third party accessed and copied certain data from their systems. Gold Reserve then conducted a manual review of the impacted data to identify individuals whose personal information was contained in the data.

On June 21, 2024, Gold Reserve completed its review of the data and identified the personal information belonging to current and former employees, Directors and consultants, including: name; date of birth; and Social Security number.

Today, July 30, 2024, Gold Reserve will begin sending notification letters via First Class Mail to 1 (one) Maryland resident. A sample copy of the notice letter is attached. Gold Reserve is offering 12 months of complimentary credit monitoring and fraud protection services to this individual through Equifax. Gold Reserve is also providing a toll-free hotline for the individual to call with any questions regarding the incident.

To help prevent a similar type of incident from occurring in the future, Gold Reserve implemented additional security protocols designed to enhance the security of its network, internal systems and applications. Gold Reserve also continues to evaluate additional steps that may be taken to further increase its defenses.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Sincerely,

Will Daugherty

GOLD RESERVE
Gold Reserve Inc
999 W. Riverside Ave.,
Suite 401
Spokane, WA 99201

July 30, 2024

00695-ADFFIN G0261 L001 AUTO *000003
MT247T5012
000003

[SAMPLE NAME]
[SAMPLE ADDRESS]

Dear [SAMPLE NAME]:

Re: Notice of Data Breach

Gold Reserve Inc. takes privacy and security seriously. Regrettably, we are writing to inform you of a cybersecurity incident we recently experienced and which may have implications for certain of your personal information. This letter sets out the steps we have taken to bolster the protection of personal information in our systems and the steps you can take personally to protect your information.

What Happened?

On April 22, 2024, we discovered that an unauthorized third party gained access to a portion of our IT infrastructure. We immediately deployed countermeasures to secure our network and data from further unauthorized access and engaged third party cybersecurity experts to assist with containment, remediation, and to conduct a forensic investigation to determine the nature and extent of the incident. The forensic investigation determined that on the same day, the unauthorized third party accessed and copied certain data from our systems. We conducted a manual review of the impacted data to identify individuals whose personal information was contained in the data. Since then, we have been working with our advisors to confirm the details of this information and collect contact information.

What Information Was Involved?

On or around June 21, 2024, we completed our review of the impacted data and determined that it contained some of your personal information, including your: Social Security Number; Personal Address; Passport; WA Driver's License.

At this time, we are not aware of any personal information being further disclosed or misused such as to carry out identity theft and/or fraud.

What Are We Doing?

In addition to retaining third-party cybersecurity experts to assist with containment, remediation and to conduct a forensic investigation, we have also reported this incident to law enforcement.

Furthermore, to provide peace of mind, we are providing impacted current and former employees, Directors and consultants with a complimentary 12 month subscription for credit monitoring through Equifax, the details of which are set out below.

00695-ADFFIN-G0261-L001 AUTO_000003-000009-000-1/2
MT247T5012

What You Can Do

Activate your complimentary credit monitoring – Through Equifax, we have arranged a 12 month complimentary subscription to Equifax Complete™ Premier.

We encourage you to take advantage of this service by enrolling online. To activate your service, please visit:

www.equifax.com/activate

You will be prompted to enter your unique activation code **353403375099** then click "Submit" and follow these 4 steps:

1. **Register**: Complete the form with your contact information and click "Continue". *If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4*.

2. **Create Account**: Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity**: To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout**: Upon successful verification of your identity, you will see the Checkout Page. Click 'Sign Me Up' to finish enrolling. The confirmation page shows your completed enrollment.

Please ensure that you redeem your activation code before 11/30/2024 to take advantage of the service.

Upon completion of the online activation process, you will have access to the following features:

- Annual access to your 3-bureau credit report and VantageScore[1] credit scores
- Daily access to your Equifax credit report and 1-bureau VantageScore credit score
- 3-bureau credit monitoring[2] with email notifications of key changes to your credit reports
- WebScan notifications[3] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[4], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[5]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[6].
- Lost Wallet Assistance if your wallet is lost or stolen, and one-stop assistance in canceling and reissuing credit, debit and personal identification cards.

FOR MORE INFORMATION

The security of your personal information is important to us. If you have any questions or need additional information, please contact Debbie Van Driel at 506-623-1500 ext. 7014.

Sincerely,

David P. Onzay
Chief Financial Officer

[1]The credit scores provided are based on the VantageScore® 3.0 model. For three-bureau VantageScore credit scores, data from Equifax®, Experian®, and TransUnion® are used respectively. Any one-bureau VantageScore uses Equifax data. Third parties use many different types of credit scores and are likely to use a different type of credit score to assess your creditworthiness.

[2]Credit monitoring from Experian and TransUnion will take several days to begin.

[3]WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[4]The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[5]Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[6]The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL INFORMATION

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, 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 reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. 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.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. 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, 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.

Federal **Trade Commission and State Attorneys General Offices.** 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 and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

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

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697-1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

For Texas residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free)

Reporting of identity theft and obtaining a police report.
You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

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 have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.