
To Maryland Attorney General,

Sun Valley Gold LLC recently discovered a data breach that may have involved personal information of a Maryland resident.

On December 5, 2024, a third party attacked our email system and obtained unauthorized, remote access to the system. This attack occurred through a password hack due to the reuse of an old password. The third party had access to the email system for approximately nine hours before being removed.

Our investigation determined that the impacted information included, among other things, investor names, email addresses, phone numbers, and brokerage account information (including account numbers).

Our investigation indicated that one Maryland resident had personal information that may have been compromised as a result of this breach. A copy of the notice being sent to this resident is attached.

We responded to the incident immediately upon discovery and took steps to ensure the security of our systems. These steps included changing the password of the affected email account and sending out an alert to all employees requiring them to strengthen their passwords and not re-use passwords. We are confident that the bad actors can no longer access the affected email account and that future attackers will not be able to obtain unauthorized access to our systems.

Sincerely,

Lara Stone
Chief Operating Officer

SUN VALLEY GOLD LLC
620 Sun Valley Road, 2nd Floor | PO Box 2211 | Ketchum, ID 83340
Email: laras@svgold.com | Phone: 208-726-2327 x3

December 20, 2024

Dear [Investor Name]:

We are writing to inform you of an incident potentially involving some of your personal information that we hold. While we are not aware of any actual or attempted misuse of your information, we are providing you with an overview of the incident and resources available to you right now to protect yourself from any consequences. (This notification has not been delayed because of a law enforcement investigation.)

What Happened

On December 5, 2024, a third party attacked our email system and obtained unauthorized, remote access to the system. The third party had access to the email system for approximately nine hours before being removed.

What Information Was Involved

Our investigation determined that the impacted information included, among other things, investor names, email addresses, phone numbers, and brokerage account information (including account numbers).

What We Are Doing

We responded to the incident immediately upon discovery and took steps to ensure the security of our systems. We are confident that the bad actors can no longer access the email account and have taken steps to ensure the continuing integrity of your personal information and to prevent future attackers from obtaining unauthorized access to our systems.

Please read the important information provided in the attachment, which contains information about steps you can take to protect yourself from the possibility of identity theft.

If you have any questions or if there is anything we can do to further assist you, please contact Lara Stone at laras@svgold.com or 208-726-2327 x3.

Sincerely,

Peter Palmedo

President

SUN VALLEY GOLD LLC

620 Sun Valley Road, 2nd Floor | PO Box 2211 | Ketchum, ID 83340

Email: peter@svgold.com | Main: 208-726-2327

Confidentiality Notice: This email (including attachments) is intended only for the person to whom it is addressed and may contain confidential information. If you are not the intended recipient, please do not read, copy or distribute this email. Please

notify the sender immediately by return email and delete it from your computer. This email should not be construed as an offer to buy or sell securities.

Data Breach - What You Can Do

Fraud Alerts

To protect yourself from the possibility of identity theft, we recommend that you evaluate placing a fraud alert on your credit files. A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for 90 days. To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to obtain a free copy of your credit report from each.

Equifax Information Services may be reached at: P.O. Box 740256, Atlanta, GA 30374. To order a credit report from Equifax, call (800) 685-1111. To place a fraud alert, call (888) 766-0008 or go to www.fraudalert.equifax.com.

Experian Security Assistance may be reached at: P.O. Box 9554, Allen, TX 75013-2002. To order a credit report or to place a fraud alert with Experian, call (888) 397-3742 or go to www.experian.com.

TransUnion Fraud Victim Assistance Center may be reached at: P.O. Box 2000, Chester, PA 19016. To order a credit report from TransUnion, call (877)322-8228. To place a fraud alert, call (800) 680-7289. To place a security freeze, call (888) 909-8872. You may also go to www.transunion.com.

Security Freezes

You may consider placing a Security Freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a 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 access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed above.

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

If you request a credit freeze online or by phone, then the credit reporting agencies have one business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three business days after getting your request.

Review Credit Reports

When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. You should also call your local police department and file a report of identity theft. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

Even if you do not find signs of fraud on your credit reports, we recommend that you remain vigilant in reviewing your credit reports from the three major credit reporting agencies listed above. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing to:

Annual Credit Report Request Service,
P.O. Box 105281
Atlanta, GA 30348-5283

For More Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General (for more information on state-specific resources, please consult the Appendix attached to this letter.)

The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; and 202-326-2222 (General Line). The Federal Trade Commission also permits those who discover that their information has been misused to file a complaint with them using the contact information listed above.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General.

You may also visit the Securities and Exchange Commission Office of Investor Education and Advocacy's website (<https://www.sec.gov/spotlight/cybersecurity>) for more information about identity theft.

Appendix

Additional Information for Residents of:

California

For additional information on protection against identity theft you may contact the California Office of Privacy Protection at www.oag.ca.gov/privacy.

Connecticut

For more information on identity theft, you may visit the Connecticut Office of the Attorney General at <https://portal.ct.gov/ag/consumer-issues/identity-theft/identity-theft>.

Florida

For more information on identity theft, you may visit the Florida Office of the Attorney General, Consumer Protection Division's website at <https://www.myfloridalegal.com/consumer-protection>.

Illinois

For more information on identity theft, you may visit the Office of the Illinois Attorney General's Consumer Protection Division website at <https://illinoisattorneygeneral.gov/consumer-protection/>.

Maryland

For more information on identity theft, you may visit the Maryland Office of the Attorney General's website at <https://www.marylandattorneygeneral.gov/>. The toll-free number for the Attorney General's office is 1-888-743-0023 and the address is 200 St. Paul Place, Baltimore, MD 21202.

Nevada

For more information on identity theft, you may visit the Nevada Attorney General's Bureau of Consumer Protection website at https://ag.nv.gov/About/Consumer_Protection/Bureau_of_Consumer_Protection/.

New York

For more information on identity theft, you may visit the following websites:

- New York Department of State Division of Consumer Protection: <https://dos.nysits.acsitefactory.com/consumer-protection>; (800) 697-1220 (Consumer Helpline)
- NYS Attorney General: <http://www.ag.ny.gov/home.html>; (800) 771-7755 (Information and Complaint Helpline)

- New York Department of Financial Services:
https://www.dfs.ny.gov/consumers/scams_schemes_frauds/security_breach; (800) 342-3736
(Consumer Questions Line).

For more information on placing a security freeze on your credit reports, please go to the New York Department of State Division of Consumer Protection website at <https://dos.nysits.acsitefactory.com/consumer-protection>.

Texas

For more information on identity theft, you may visit the Attorney General of Texas' website at <https://www.texasattorneygeneral.gov/consumer-protection/identity-theft>.