BRACEWELL

July 16, 2021

BY EMAIL

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Breach Notification

To Whom it May Concern:

On behalf of Asarco LLC, I am writing to notify your office of an incident that may affect the security of personal information of New Hampshire residents.

On March 1, 2021, Asarco LLC experienced a breach of its information security systems by a malicious third party. The attacker deployed ransomware and encrypted some of Asarco's servers in the United States and Mexico. Asarco refused to pay the hackers, instead focusing solely on investigating the hack and securing its systems. After remediating and restoring affected servers, Asarco and its outside experts continued forensic monitoring and, on May 3, 2021, discovered that some data from Asarco's servers had been made public without authorization.

Upon discovery of the incident on March 1, Asarco immediately began a remediation and recovery process. Asarco quickly disconnected its servers, deactivated the access point used to deploy the malicious program, and isolated the Data Center. Asarco is working with a leading cybersecurity firm that is analyzing the malware used in the attack on Asarco and is monitoring the dark web to identify any additional data that might have been compromised. Asarco is making enhancements to internal security systems and implementing additional procedures to mitigate future risk.

Approximately 4 New Hampshire residents were affected by the breach. Affected New Hampshire residents were notified on July 16, 2021. Attached is a sample of the notification made to affected individuals.

Very truly yours,

Philip J. Bezanson
Managing Partner, Seattle

Philip J. Bezanson
Managing Partner, Seattle
T: +1.206.204.6206 F: +1.800.404.3970
701 Fifth Avenue, Suite 6200, Seattle, Washington 98104-7018
philip.bezanson@bracewell.com bracewell.com

GrupoMéxico MINING

ASARCO

Notice of Data Breach

[INDIVIDUAL NAME]
[STREET ADDRESS]
[CITY, STATE AND POSTAL CODE]
[DATE]

Dear [INDIVIDUAL NAME]:

We are writing to notify you of a data security incident that might have impacted your personal information. We take the protection of your information very seriously and are contacting you directly to explain the circumstances surrounding the incident, the steps we are taking in response, and the resources we are making available to you.

What Happened?

On March 1, 2021, Asarco LLC experienced a breach of its information security systems by a malicious third party. The attacker deployed ransomware and encrypted some of Asarco's servers in the United States and Mexico. After remediating and restoring affected servers, Asarco and its outside experts continued forensic monitoring and, on May 3, 2021, discovered that some data from Asarco's servers had been made public without authorization.

What information is involved?

Based on what we have learned so far, the information on our servers that may have been compromised includes names, financial account information, social security numbers, driver's license numbers, health insurance policy numbers, dates of birth, ATF licensing information, medical information affiliated with workers compensation claims, and personal information affiliated with retirement accounts, retirement benefits, or retirement accounts or benefits for which you are listed as a spouse, dependent, or beneficiary.

What are we doing?

Upon discovery of the incident on March 1, Asarco immediately began a remediation and recovery process. Asarco quickly disconnected its servers, deactivated the access point used to deploy the malicious program, and isolated the Data Center. Asarco is working with a leading cybersecurity firm that is analyzing the malware used in the attack on Asarco and is monitoring the dark web to identify any additional data that might have been compromised. Asarco is making enhancements to internal security systems and implementing additional procedures to mitigate future risk.

As an added precaution, we have arranged to have NortonLifeLock to protect your identity and monitor your credit for 12 months at no cost to you. To activate your membership online and get protection at no cost to you:

1. In your web browser, go directly to [redacted] Click on the yellow "START MEMBERSHIP" button (*do not attempt registration from a link presented by a search engine).*

2. You will be taken to another page where, below the FOUR protection plan boxes, you may enter the [redacted] and click the "APPLY" button.

3. On the next screen, enter your [redacted] and click the "APPLY" button.

4. Your complimentary offer is presented. [redacted] button.

5. Once enrollment is completed, you will receive a confirmation email (*be sure to follow ALL directions in this email*).

Alternatively, to activate your membership over the phone, please call: 1-800-899-0180. When you call, make sure to have this notice letter in-hand.

You will have until 9/20/21 to enroll in this service.

What can you do?

We want to make sure you are aware of steps you can take to guard against potential identity theft or fraud. Please review the enclosed guidance from the U.S. Federal Trade Commission (FTC) for information about what you can do to protect yourself from identity theft.

Under federal law, you are entitled to one free copy of your credit report annually. Visit www.annualcreditreport.com, call toll-free at 1-877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission (FTC) website at www.ftc.gov.

The FTC recommends that you place a free fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Contact any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for one year. You can renew it after one year.

Equifax	**Experian**	**TransUnion**
Equifax Information Services LLC	Credit Fraud Center	Fraud Victim Assistance Department
P.O. Box 105069	P.O. Box 9701	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19016
www.equifax.com/personal/credit-report-services	www.experian.com/help	www.transunion.com/credit-help
1-800-525-6285	1-888-397-3742	1-800-680-7289

Ask each credit bureau to send you a free credit report after it places a fraud alert on your file. Review your credit reports for accounts and inquiries you don't recognize. These can be signs of identity theft. If your personal information has been misused, visit the FTC's website at IdentityTheft.gov to report the identity theft and get recovery steps. Even if you do not find any suspicious activity on your initial credit reports, the FTC recommends that you check your credit reports periodically so you can spot problems and address them quickly.

You may also want to consider activating a free credit freeze. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. To place a freeze, contact each of the major credit bureaus at the links or phone numbers above. A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it.

If you find suspicious activity on your credit reports or have reason to believe your information has been misused, you should file a police report, and retain a copy of the report, since many creditors want the information it contains to absolve you of any fraudulent debts. If you have questions about contacting law enforcement personnel, you can direct them to the Asarco Data Breach Hotline. You also should file a complaint with the FTC via the web at www.ftc.gov/idtheft, by phone at 1-877-ID-THEFT (877-438-4338), or by mail to the Federal Trade Commission, Bureau of Consumer Protection, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement to aid in criminal investigations.

You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; the right to ask for a credit score; the right to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

For more information

If you have further questions or concerns about this incident, please email notification@asarco.com or call the Asarco Data Breach Hotline at 520-798-7509 Monday through Friday, 8am – 8 pm CT. Please see the following page for certain state-specific information.

We sincerely regret any inconvenience or concern caused by this incident.

Sincerely,

Oscar Gonzalez

VP/CFO, ASARCO LLC

IF YOU ARE A D.C. RESIDENT:

You may obtain information about avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001; (202) 727-3400; https://oag.dc.gov/

IF YOU ARE AN IOWA RESIDENT:

You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached at: Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319; (515) 281-5164; www.iowaattorneygeneral.gov

IF YOU ARE A MARYLAND RESIDENT:

You may obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at: Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; www.marylandattorneygeneral.gov

IF YOU ARE A NEW YORK RESIDENT:

You may contact and obtain information about preventing identity theft from the New York State Division of Consumer Protection. This office can be reached at: New York State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001; (518) 474-8583 / (800) 697-1220; http://www.dos.ny.gov/consumerprotection

You may also contact the New York State Attorney General's Office. This office can be reached at: New York State Attorney General's Office, The Capitol, Albany, NY 12224-0341; (800) 771-7755; https://ag.ny.gov/

IF YOU ARE A NORTH CAROLINA RESIDENT:

You may obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6000; http://www.ncdoj.gov

IF YOU ARE AN OREGON RESIDENT:

You may obtain information about preventing identity theft from the Oregon Attorney General's Office. This office can be reached at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; (877) 877-9392; http://www.doj.state.or.us

IF YOU ARE A RHODE ISLAND RESIDENT:

You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at: Rhode Island Office of Attorney General, 150 South Main Street, Providence, Rhode Island 02903; (401) 274-4400; http://www.riag.ri.gov

FEDERAL TRADE COMMISSION
IdentityTheft.gov

What information was lost or exposed?

Social Security number

- [ ] If a company responsible for exposing your information offers you free credit monitoring, take advantage of it.
- [ ] Get your free credit reports from annualcreditreport.com. Check for any accounts or charges you don't recognize.
- [ ] Consider placing a credit freeze. A credit freeze makes it harder for someone to open a new account in your name.
  - If you place a freeze, be ready to take a few extra steps the next time you apply for a new credit card or cell phone – or any service that requires a credit check.
  - If you decide not to place a credit freeze, at least consider placing a fraud alert.
- [ ] Try to file your taxes early — before a scammer can. Tax identity theft happens when someone uses your Social Security number to get a tax refund or a job. Respond right away to letters from the IRS.
- [ ] Don't believe anyone who **calls** and says you'll be arrested unless you pay for taxes or debt — even if they have part or all of your Social Security number, or they say they're from the IRS.
- [ ] Continue to check your credit reports at annualcreditreport.com. You can order a free report from each of the three credit reporting companies once a year.

Online login or password

- [ ] Log in to that account and change your password. If possible, also change your username.
  - If you can't log in, contact the company. Ask them how you can recover or shut down the account.
- [ ] If you use the same password anywhere else, change that, too.
- [ ] Is it a financial site, or is your credit card number stored? Check your account for any charges that you don't recognize.

Debit or credit card number

- [ ] Contact your bank or credit card company to cancel your card and request a new one.
- [ ] Review your transactions regularly. Make sure no one misused your card.
  - If you find fraudulent charges, call the fraud department and get them removed.
- [ ] If you have automatic payments set up, update them with your new card number.
- [ ] Check your credit report at annualcreditreport.com.

Bank account information

- [ ] Contact your bank to close the account and open a new one.
- [ ] Review your transactions regularly to make sure no one misused your account.
  - If you find fraudulent charges or withdrawals, call the fraud department and get them removed.
- [ ] If you have automatic payments set up, update them with your new bank account information.
- [ ] Check your credit report at annualcreditreport.com.

Driver's license information

- [ ] Contact your nearest motor vehicles branch to report a lost or stolen driver's license. The state might flag your license number in case someone else tries to use it, or they might suggest that you apply for a duplicate.
- [ ] Check your credit report at annualcreditreport.com.

Children's personal information

- [ ] Request a credit freeze for your child — if this service is available in your state. A credit freeze will make it difficult for someone to use your child's information to open accounts. To place a freeze, follow the specific instructions for each credit bureau:

- Equifax
- Experian
- Transunion

- [ ] No matter what state you live in, you can check to see if your child has a credit report. Each bureau has specific instructions for these requests:

  - Equifax
  - Experian (Click on "Minor Child Instructions" under "Information You Should Know")
  - Transunion

- [ ] If a credit bureau has a credit report for your child, the credit bureau will send you a copy of the report. Use the instructions provided with the credit report to remove fraudulent accounts.

- [ ] Review the FTC's information on Child Identity Theft.