Substitute Notice of Data Breach

January 6, 2022

Earlier this year, we informed current employees, former employees, and the spouses, dependents, and beneficiaries of current and former employees that ASARCO LLC ("ASARCO") was subject to a malicious cyberattack. On July 16, 2021, we completed mailing individual notices to their current physical addresses, whenever possible. This post provides updated information on the impact of the cyber-attack and our response.

What Happened?

On March 1, 2021, ASARCO 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 attack 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.

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; other government identification numbers; dates of birth; a limited number of usernames and passwords; ATF licensing information; medical information affiliated with workers compensation claims; and personal information affiliated with ASARCO Health, Dental, Vision, Flexible Spending, and Retiree Health and Prescription Plans, such as names, addresses, dates of birth, social security numbers, claims information, bank account numbers, and a limited amount of clinical information.

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 has been 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.

Once ASARCO information was discovered on the dark web, ASARCO initiated a comprehensive review, with the assistance of industry leading forensic specialists, to identify any personally identifying information in the impacted systems. That third-party review, which involved a large, complex data set, was completed in December 2021. ASARCO then undertook a comprehensive internal reconciliation of the records found to identify individuals and confirm contact information. That review is now complete, and ASARCO is in the process of mailing notice letters to available current addressees for all newly identified individuals whose data may have been compromised in the attack.

ASARCO has taken steps to protect against future breaches of personal information, including a range of technical safeguards, such as strengthened firewalls, additional multi-factor authentication, and new encryption technologies, as well as changing all system passwords. ASARCO is also making enhancements to internal security systems and implementing additional procedures to mitigate future risk.

As an added precaution, ASARCO has arranged to have NortonLifeLock protect potentially affected individuals' identity and monitor their credit for 12 months at no cost. If you believe you may have been affected and have not yet had an opportunity to enroll in the free credit monitoring and identity theft protection services, please email notification@asarco.com or call the ASARCO Data Breach Hotline at 520-798-7509 Monday through Friday, 8am – 5 pm CT.

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. For more information about what you can do to protect yourself from identity theft, please refer to guidance from the U.S. Federal Trade Commission (FTC) on their website: https://www.identitytheft.gov/#/Info-Lost-or-Stolen

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
P.O. Box 105069	P.O. Box 9701	Department
Atlanta, GA 30348-5069	Allen, TX 75013	P.O. Box 2000
www.equifax.com/personal/credit-report-services	www.experian.com/help	Chester, PA 19016
1-800-525-6285	1-888-397-3742	www.transunion.com/credit-help
		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.

Finally, if you still use the same usernames and passwords that you used in 2017 or earlier for any account or website, we strongly recommend that you change your passwords. Reusing passwords, or using weak passwords, makes it easier for attackers to steal your information, particularly if you re-use a potentially compromised password.

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 below for certain state-specific information.

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

CALIFORNIA RESIDENTS: Visit the California Office of Privacy Protection for additional information on protection against identity theft: https://oag.ca.gov/privacy

D.C. RESIDENTS: 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/

IOWA RESIDENTS: 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

KENTUCKY RESIDENTS: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: +1 (502) 696-5300.

MARYLAND RESIDENTS: 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

MASSACHUSETTS RESIDENTS: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

NEW YORK RESIDENTS: 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/

NORTH CAROLINA RESIDENTS: 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

OREGON RESIDENTS: 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

RHODE ISLAND RESIDENTS: 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