

October 30, 2024

ELECTRONIC MAIL

Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202
idtheft@oag.state.md.us

Re: Notice of Security Incident

To Whom It May Concern:

We write on behalf of Sierra Construction Company (“Sierra Construction”) to notify your office of a recent data incident involving personal information relating to four (4) Maryland residents.

On or around August 14, 2024, Sierra Construction became aware of a security incident impacting a portion of its environment. Sierra Construction promptly launched an investigation and determined that the activity resulted from a cybersecurity incident.

Upon discovery of the incident, Sierra Construction immediately initiated measures to secure the information it maintains. Sierra Construction also engaged the services of outside legal counsel, engaged external cybersecurity experts to investigate the nature and scope of the incident, and conducted an investigation to determine what information was involved.

The information involved varies depending on the individual and their relationship with Sierra Construction. However, the following types of information were potentially involved in this incident: name, address, date of birth, Social Security number, government identifiers (e.g. driver’s license, state identification, or passport number), health insurance information, and/or pre-employment test results.

In response to the incident, Sierra Construction will be providing affected consumers with complimentary identity protection services and has implemented additional safeguards, including the adoption of encryption technologies, changing passwords, strengthening password requirements, and deploying additional security tooling in its environment.

Attached as **Exhibit A** is sample of the consumer notification letter for your reference. Should you have any questions or concerns about this matter, please do not hesitate to contact me using the information provided below.

Sincerely,

A handwritten signature in black ink, appearing to read 'Sadia Mirza'.

Sadia Mirza
Direct: 949.622.2786
Email: sadia.mirza@troutman.com

EXHIBIT A

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

Enrollment Code: <<Activation Code>>

To Enroll Visit:

<https://www.experianidworks.com/3bcredit>

Or

Call: (877) 288-8057

Enrollment Deadline: <<Enrollment
Deadline>>

<<Date>>

Notice of Data Breach

Dear <<Full Name>>,

Sierra Construction Company ("Sierra Construction") is writing to inform you of a recent security incident involving your personal information. We encourage you to read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened?

On or around August 14, 2024, Sierra Construction became aware of a security incident impacting a portion of our environment. We promptly launched an investigation and determined that the activity resulted from a cybersecurity incident.

What Information was Involved?

Sierra Construction may have your information because you are a current or former employee of the company.

While the specific information varies by individual, certain employment-related details may have been involved, including but not limited to your name, date of birth, Social Security number, government identifiers (e.g., driver's license, state identification, or passport number), health insurance information, and/or pre-employment test results.

Additionally, if you provided information about your dependents and beneficiaries during your employment, their information might also be affected. For further details and to access resources specifically available to your dependents and beneficiaries, please contact our dedicated toll-free number for this incident.

It's possible that your dependents and beneficiaries will receive a separate letter. Please be assured that the letter is legitimate and relates to this incident, which we are notifying you about separately.

What Are We Doing.

Upon discovery of the incident, we immediately initiated measures to secure the information we maintain. We also engaged the services of outside legal counsel, engaged external cybersecurity experts to investigate the nature and scope of the incident, and investigated to determine what information was involved.

What Can You Do?

We are encouraging individuals to take steps to protect their personal information and are also offering affected individuals with 12 months of complimentary access to Experian IdentityWorksSM. Additional information pertaining to these services and enrollment instructions are provided below.

1. **Register for Identity Protection Services.** We are offering complimentary access to Experian IdentityWorks for 12 months. These services provide access to the following:

- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** This service provides restoration services for identity theft issues. Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Identity Theft Insurance:** This service provides coverage for certain costs and unauthorized electronic fund transfers.

Enrollment Instructions: Using your unique activation code, <<Activation Code>>, you may enroll in the service in two ways:

- Online: Visit <https://www.experianidworks.com/3bcredit> and follow the instructions to enroll. Please note that you will be asked to create an account and complete an identity verification process to enroll in the service.
- By Phone: We encourage you to contact Experian with any questions about Experian IdentityWorks or how to enroll by calling (877) 288-8057. Experian representatives are available Monday through Friday from 8 AM to 8 PM Central Time. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the Identity Restoration services by Experian.

If you have questions regarding the incident or this notice letter, please do not hesitate to contact 855-277-7702.

2. **Review Your Accounts for Suspicious Activity.** We encourage you to remain vigilant by regularly reviewing your accounts and monitoring credit reports for suspicious activity.
3. **Order a Credit Report.** If you are a U.S. resident, you are entitled under U.S. law to one free credit report annually from each of the three nationwide consumer reporting agencies. To order your free credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit reporting agency delete that information from your credit report file. Contact information for the nationwide credit reporting agencies is provided in the next section.
4. **Contact the Federal Trade Commission, Law Enforcement and Credit Bureaus.** You may contact the Federal Trade Commission ("FTC"), your state's Attorney General's office, or law enforcement, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's websites at www.identitytheft.gov and; call the FTC at (877) IDTHEFT (438-4338); or write to: FTC Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may contact the nationwide credit reporting agencies at:

- a) **Equifax:** (800) 525-6285; P.O. Box 740241, Atlanta, Georgia, 30374; or www.equifax.com.
 - b) **Experian:** (888) 397-3742; P.O. Box 9701, Allen, TX 75013; or www.experian.com.
 - c) **TransUnion:** (800) 916-8800; Fraud Victim Assistance Division, P.O. Box 2000, Chester, PA 19022; or www.transunion.com.
5. **Additional Rights Under the FCRA.** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here.

Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by: (i) visiting https://files.consumerfinance.gov/f/documents/bcfc_consumer-rights-summary_2018-09.pdf ; or (ii) by writing to Consumer Financial Protection Bureau, 1700 G Street, N.W., Washington, DC 20552.

6. **Request Fraud Alerts and Security Freezes.** You may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and security freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file. In addition, you can contact the nationwide credit reporting agencies at the following numbers to place a security freeze at no cost to you:

- a) Equifax: (800) 349-9960
- b) Experian: (888) 397-3742
- c) TransUnion: (888) 909-8872

Placing a security freeze prohibits the agency from releasing any information about your credit report without your written authorization. Security freezes must be placed separately at each of the three nationwide credit reporting agencies. When requesting a security freeze, you may need to provide the following information:

- Your full name, with middle initial as well as Jr., Sr., II, etc.
- Social Security number
- Date of birth
- Current address and all addresses for the past two years
- Proof of current address, such as a current utility bill or telephone bill
- Legible copy of a government-issued identification card, such as a state driver's license, state identification card, or military identification.

After receiving your request, each agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

Other Important Information

7. **For Maryland Residents.** You can obtain information about avoiding identity theft from the Maryland Attorney General at: Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202, (888) 743-0023 (toll-free in Maryland), (410) 576-6300, www.marylandattorneygeneral.gov.
8. **For New York Residents.** You can obtain information about security breach response, identity theft prevention, and identity protection information from the New York State Office of the Attorney General at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755 (toll-free), 1-800-788-9898 (TDD/TTY toll-free line), <https://ag.ny.gov/>, and at: Bureau of Internet and Technology (BIT), 28 Liberty Street, New York, NY 10005, Phone: (212) 416-8433, <https://ag.ny.gov/internet/resource-center>.
9. **For North Carolina Residents.** You can obtain information about avoiding identity theft from the North Carolina Attorney General at: North Carolina Attorney General's Office 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov.
10. **For Residents of Oregon.** You may report suspected identity theft to law enforcement, including the Office of the Oregon Attorney General and the FTC. Contact information for the FTC is included in your notice. The Office of the Oregon Attorney General can be reached: (1) by mail at 1162 Court St. NE, Salem, OR 97301; (2) by phone at (877) 877-9392; or (3) online at <https://www.doj.state.or.us/>.
11. **For Rhode Island Resident.** You can obtain information about avoiding identity theft from the Rhode Island Office of the Attorney General at: Rhode Island Office of the Attorney General, Consumer Protection Unit 150, South Main Street, Providence, RI 02903, (401)-274-4400, www.riag.ri.gov. You have the right to obtain a police report, and to request a security freeze (charges may apply), as described above. Information pertaining to approximately 1 Rhode Island resident was potentially involved in this incident.

For More Information.

If you have any questions or concerns, please do not hesitate to contact 855-277-7702, Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time, (excluding major U.S holidays).

Sincerely,

Nancy Adler
Director of Corporate Administration