

Cornerstone Staffing Solutions, Inc.
c/o Return Processing Center:
555 Monster Rd SW | Renton, WA 98057

PRESORT
FIRST-CLASS MAIL
US POSTAGE
PAID
CHICAGO, IL
PERMIT NO 4187

Via First-Class Mail

<<FIRST NAME>> <<LAST NAME>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>
<<Country>>

September 11, 2026

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>,

Cornerstone Staffing Solutions, Inc. (“Cornerstone”) is writing to inform you about a data breach that may have affected the security of your personal information. This letter explains what happened, what Cornerstone is doing in response, and the steps you can take to help protect your information.

What Happened?

On or about November 17, 2025, Cornerstone detected anomalous activity indicative of a potential data security incident wherein an unauthorized actor may have gained access to portions of the company’s network environment. Upon becoming aware of the incident, Cornerstone immediately launched an internal investigation and, at the direction of counsel, engaged a third-party cybersecurity firm to contain the threat, support the investigation, and determine the scope of the unauthorized access.

The investigation was unable to identify the root cause of the incident. However, the investigation found indications that certain Cornerstone systems may have been accessed without authorization between November 6 and 21, 2025, and that some data may have been removed from the environment, although the specific files involved could not be determined with certainty. After identifying the potentially affected areas of the environment, Cornerstone worked diligently with a third-party vendor, through counsel, to review the information that was present in those areas, identify the individuals whose personal information was among that data, and confirm the types of personal information potentially involved. These efforts were completed on August 7, 2026. Because it could not be determined with certainty whether any specific personal information was actually accessed or acquired by the unauthorized actor, Cornerstone is providing notice of the incident out of an abundance of caution to all individuals whose information was present in the affected environment.

What Information Was Involved?

Based on the investigation to date, the following types of personal information were maintained on the affected environment: name, <<Breached Elements>>. *Please note that receipt of this notice does not mean that your information was actually accessed and/or acquired by the unauthorized third party.* To date, Cornerstone has not received any reports from individuals that their personal information has been used for identity theft.

What We Are Doing

As described above, upon detecting the anomalous activity, Cornerstone immediately launched an investigation and engaged a third-party cybersecurity firm to contain the threat and determine the scope of the potential unauthorized access. Cornerstone has implemented additional security measures and is continuing to evaluate ways to further enhance the security of its environment to minimize the likelihood of similar events occurring in the future.

As an added precaution, Cornerstone is offering you <<CM Duration>> months of complimentary credit monitoring and identity protection services through HaystackID, a company specializing in these services. Instructions for how to enroll in these services are below.

What You Can Do

As a precautionary measure, Cornerstone encourages you to remain vigilant against identity theft and fraud by regularly reviewing your account statements with all of your financial institutions. You may also choose to monitor your credit reports. The resources guide enclosed with this letter describes additional steps you can take and provides contact details for the Federal Trade Commission and credit reporting agencies, as well as information on how to place fraud alerts and security freezes.

To enroll in Credit Monitoring services at no charge, please log on to the following and follow the instructions provided: **www.equifax.com/activate**.

When prompted please provide the following activation code to receive services: <<Activation Code>>.

In order for you to receive the monitoring services described above, you must enroll within ninety (90) days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

If you have any questions or concerns not addressed in this letter, please call 866-210-2106 (toll free) Monday through Friday, during the hours of 9:00 a.m. and 9:00 p.m. Eastern Standard Time (excluding U.S. national holidays). Please have this letter ready if you call.

Sincerely,

Cornerstone Staffing Solutions, Inc.

Steps You Can Take to Further Protect Your Information

1. Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC).

We recommend that you review the tips provided by the FTC's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf. The FTC can also be reached at: 600 Pennsylvania Avenue, NW, Washington, DC 20580; and (202) 326-2222.

2. Obtain and Monitor Your Credit Report

You are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

3. Consider Placing a Fraud Alert on Your Credit Report

At no charge, you can also have these credit bureaus place an initial "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax

1-888-378-4329

P.O. Box 105069

Atlanta, GA 30348-5069

<https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Experian

1-888-397-3742

P.O. Box 9554

Allen, TX 75013-9544

www.experian.com/fraud/center.html

TransUnion

1-800-916-8800

P.O. Box 2000

Chester, PA 19016

www.transunion.com/fraud-victim-resource/place-fraud-alert

4. Security Freeze

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit,

mortgages, employment, housing, or other services. Under federal law, you cannot be charged to place, lift, or remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all your credit files. To find out more on how to place a security freeze, you can use the contact information provided below.

Equifax

1-888-298-0045

P.O. Box 105788

Atlanta, GA 30348-5788

www.equifax.com/personal/credit-report-services/credit-freeze/

Experian

(888) 397-3742

P.O. Box 9554

Allen, TX 75013-9544

<http://www.experian.com/freeze/center.html>

TransUnion

1-800-916-8800

P.O. Box 160

Woodlyn, PA 19094

www.transunion.com/credit-freeze

To request a security freeze, you will need to provide some or all the following information to the credit reporting agency, depending on whether you do so online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security Number
3. Date of Birth
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Social Security Card, pay stub, or W2
8. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Credit reporting agencies have one (1) to three (3) business days after receiving your request to place a security freeze on your credit report, based upon the method of your request. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password (or both) that can be used by you to authorize the removal or lifting of the security freeze. It is important to maintain this PIN/password in a secure place, as you will need it to lift or remove the security freeze.

You may file a police report if you ever experience identity fraud. Please note that to file a crime report or incident report with law enforcement for identity theft, you may need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement, your state Attorney General, or the Federal Trade Commission.

This notice has not been delayed by law enforcement.