

Sample Template Notice for Prolink Staffing Services, LLC

[Date]

[First Name Last Name]

[Address]

[City, State Zip]

RE: Notification of Security Incident

Dear [First Name],

Prolink Staffing Services, LLC (“Company”, “we” or “our”) takes the security and protection of your personal information seriously. This letter is in regard to an incident that our Company experienced involving the security of your personal data on its systems. We sincerely regret to inform you that the incident may have resulted in the access or viewing of your personal information. Once aware of the incident, we quickly took steps to eliminate the threat of further unauthorized access, safeguarded the information in our possession, and conducted a forensics investigation to determine the scope of the incident. While we have no reason to believe your personal information was taken or misused because of this incident, we are providing this letter to you out of an abundance of caution and to provide you information about the incident and what you can do to remain vigilant and protect your personal information.

What Happened

On or about September 6, 2025, we were notified by a trusted service provider of potentially suspicious activity involving the sending of fraudulent messages from an account owned by the Company. We immediately commenced an investigation into this activity to stop the sending of such messages, investigate the root cause of the activity and identify any other data or systems that might have been accessed as a result. Based on our investigation, the scope of this access was limited to one Company account that contained certain sensitive personal information of certain current and former Company employees. At this time, we have no evidence that any employee information has been taken or used for unauthorized purposes. We only know that, based on our investigation, such use was possible.

What Information Was Involved

The information at risk because of this incident included certain information specific to an individual’s hiring or employment with the Company. While the information may vary from person to person, generally the personal information at risk includes, but is not necessarily limited to:

First and last name	Address and phone number	Date of birth
Driver’s license number	Health information	Social Security number

What We Are Doing

Once aware of the fraudulent messaging and unauthorized access that led to it, we immediately took steps to secure the affected account and commenced a forensic investigation to understand the scope of the access and potential risks. We engaged a third-party security firm to assist in this investigation, to include assisting us with evaluating any data that might be at risk. Working with this security firm, the Company

had also identified and implemented additional administrative, technical and physical safeguards to protect against a recurrence of such unauthorized activity.

What You Can Do

Again, at this time, we have no indication that your personal information has been misused or was even the target of the unauthorized activity we discovered. Regardless, as always, you should be diligent in monitoring your personal information, including locations in which your personal information may be kept, such as bank accounts.

For More Information

If you are concerned about identity theft, you can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit bureaus at one of the phone numbers listed below or by visiting their respective websites.

Equifax 1- 800-525-6285 P.O. Box 740241 Atlanta, GA 30374 https://www.equifax.com/personal/credit-report-services/	Experian 1-888-397-3742 P.O. Box 4500 Allen, TX 75013 https://www.experian.com/help/	TransUnion 1-877-322-8228 P.O. Box 2000 Chester, PA 19016 https://www.transunion.com/credit-help
---	---	---

Credit Reports. You can request credit reports from all three credit bureaus be sent to you free of charge. Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

Fraud Alerts. You can place a fraud alert with the credit bureaus free of charge. 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. You may also place an extended fraud alert, which lasts up to seven years unless you cancel it sooner. Additionally, you can provide a phone number instructing lenders to contact you if someone applies for credit in your name, and you will get an instant alert to the potential fraud.

Security Freeze. Under state law, a security freeze (or credit freeze) prohibits a credit bureau from releasing any information from a consumer's credit report without written authorization. There is no fee associated with freezing or thawing your credit. The process of freezing your credit takes only a few minutes. You must contact each credit bureau individually to freeze your credit with each bureau. To place a security freeze, you may need to provide the following information:

Your full name	Date of Birth	Social Security number
Postal address	Email address	Other information the Credit Reporting Agency may require.

The credit bureaus have one (1) business day after your request to place a security freeze if made by telephone or secure electronic means. If the request is made by mail, the credit bureaus have three (3) business days. The credit bureaus must also send written confirmation to you within five (5) business days.

To lift the security freeze, in order to allow a specific entity or individual access to your credit report, you must apply online, call, or send a written request to the credit bureaus by mail. When you contact a credit

bureau to lift the security freeze, you will need to include proper identification (name, address, and Social Security number) and the PIN number or password that was provided to you (if provided) when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. If you request a credit thaw online or by phone, the credit bureaus are required by law to complete the request within one hour. If you request the thaw by regular mail, the credit bureaus have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

The Federal Trade Commission (FTC) provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You can also contact the FTC by using the information below.

Federal Trade Commission
1-877-438-4338
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at:

[Contact Information for Company]

Sincerely,

Prolink Staffing Services, LLC