[The Job Shop Letterhead]

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

**NOTICE OF SECURITY INCIDENT**

Dear [insert]:

We are writing to inform you of a security incident that The Job Shop experienced, which may have affected your personal information.

**What Happened?**

On August 14, 2025, a company providing IT services to The Job Shop ("Vendor") informed The Job Shop that it was the victim of a security incident. Specifically, the Vendor informed The Job Shop that, around mid-June 2025, an unknown threat actor gained unauthorized access to The Job Shop's remote desktop server ("Server") managed by the Vendor, and that the threat actor may have exfiltrated certain information from the Server.

**What Information Was Involved?**

The Server contained completed Forms W-2 for 2018, 2019, and 2020. We believe that some of these W-2 forms were likely exfiltrated; however, we are unable to determine *which* W-2 forms were exfiltrated or if *all* W-2 forms on the Server were exfiltrated.

If the exfiltrated data from the Server included *your* Form W-2, then that data would have included:

- your full name;
- your mailing address; and
- your Social Security Number.

**What We Are Doing**

- Once The Job Shop was notified of this incident, it undertook an investigation, and it retained a law firm to assist and advise The Job Shop with this investigation and its response.
- The Job Shop has taken steps to ensure that W-2 forms are protected from future malicious activity.

- The Job Shop has arranged for free credit monitoring and identity theft protection services for twenty-four months for anyone potentially affected by this exposure of W-2 forms (details below).

**What You Can Do**

As always, regularly monitor all your online accounts for unusual activity. If you observe or learn of unusual activity associated with any online account, promptly investigate the activity and take appropriate steps to protect the affected account.

Exercise caution when using the Internet to communicate or interact with any individuals you do not know; and take steps to ensure that individuals contacting you via the Internet are who they claim to be.

Review the attachment to this letter, "Steps You Can Take to Further Protect Your Information," which has further information on ways you can protect your online information, and information on how you can receive free credit monitoring and identity theft protection services for twenty-four months.

**For More Information**

If you have any questions about the security incident, you may contact us at:

The Job Shop
460 Brannan Street, #77008
San Francisco, CA, 94107
jobs@JobShopSF.com

Sincerely,

[NAME]
[TITLE]

## Steps You Can Take to Protect Your Information

- **Review Your Account Statements; Notify Law Enforcement of Any Suspicious Activity**

    - Be vigilant by closely reviewing all your account statements and credit reports.

    - If you detect suspicious account activity, promptly notify the financial institution or company that maintains the account.

    - Promptly report any suspected or actual fraudulent activity or identity theft to law enforcement (including your local police department), and consider reporting that information to your state attorney general and the Federal Trade Commission (FTC).

    - To file a complaint with the FTC, visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC are added to the FTC's Identity Theft Data Clearinghouse, a database available to law enforcement agencies.

- **Obtaining and Monitoring Your Credit Report**

You can obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months, by visiting www.annualcreditreport.com, calling 877-322-8228, or completing an *Annual Credit Report Request Form* and mailing it to:

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348

The printable request form is at:
www.annualcreditreport.com/manualRequest Form.action.

The online form is at:
https://www.annualcreditreport.com/requestReport/requestForm.action.

You can purchase a copy of your credit report by contacting any of the three national credit reporting agencies, using the following contact information:

| | **Equifax** | **Experian** | **TransUnion** |
|---|---|---|---|
| **Contact Info** | 866-349-5191<br>www.equifax.com<br>P.O. Box 740241<br>Atlanta, GA 30374 | 888-397-3742<br>www.experian.com<br>P.O. Box 2002<br>Allen, TX 75013 | 800-888-4213<br>www.transunion.com<br>2 Baldwin Place<br>P.O. Box 1000<br>Chester, PA 19016 |

- **Placing a Fraud Alert on Your Credit Report**

Consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is at www.annualcreditreport.com.

- **Credit Report Monitoring and Identity Theft Protection Services**

The Job Shop has arranged for Equifax to provide you with its *Equifax Credit Watch™ Gold* credit monitoring and identity theft protection services for twenty-four months, at no cost to you.[1]

These Services offer the following benefits:

  - Credit monitoring with email notifications of key changes to your Equifax credit report;
  - Daily access to your Equifax credit report;
  - WebScan notifications[2] when your personal information, such as Social Security Number, credit/debit card or bank account numbers, are found on fraudulent Internet trading sites;
  - Automatic fraud alerts[3], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[4];

---

[1] You must be over age 18 with a credit file to take advantage of the product.

[2] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[3] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[4] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and

- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf; and
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[5].

To take advantage of this offer, you must enroll by ***[add date]*.**

- ***Equifax Credit Watch™ Gold* Enrollment Instructions:**
  - Go to www.equifax.com/activate.
  - Enter your unique Activation Code [Activation Code]
  - Click "Submit"
  - Follow these 4 steps:
    1. **Register**. Complete the form with your contact information and click "Continue."

       If you already have a *myEquifax* account, click the *'Sign in here'* link under the *"Let's get started"* header.

       Once you have successfully signed in, skip to *Checkout Page* in Step 4.
    2. **Create Account**. Enter your email address, create a password, and accept the Terms of Use.
    3. **Verify Identity**. To enroll in your product, complete the identity verification process.
    4. **Checkout**. Upon successful verification of your identity, you will see the Checkout Page.

---

collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

[5] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

- Click 'Sign Me Up' to finish enrolling.
- The confirmation page will show your completed enrollment.
- Click "View My Product" to access the product features.

- **Take Advantage of Additional Free Resources on Identity Theft**

We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. This additional information is available at https://consumer.ftc.gov/identity-theft-and-online-security.

For more information, 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, is at https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

- **Other Important Information**
  - **Security Freeze**

In some U.S. states, you have the right to put a security freeze on your credit file. A security freeze (also known as a credit freeze) makes it harder for someone to open a new account in your name. It is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to apply for a new credit card, wireless phone, or any service that requires a credit check. You must separately place a security freeze on your credit file with each credit reporting agency. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement, or insurance statement. There is no charge to request a security freeze or to remove a security freeze.

**# # #**