[Insert date of Notice]

Fresno Regional Workforce Development Board

NOTICE OF DATA BREACH

[Insert Address]

Dear _____,

The Fresno Regional Workforce Development Board, a local public agency ("Workforce"), writes to notify you of a data security incident that may have resulted in the unauthorized access to, or acquisition of, certain personal information of yours in Workforce's possession. We take this incident very seriously and are providing you information about the incident, our response, and steps you can take to protect your personal data.

What Happened?

- Workforce was the victim of a ransomware cyberattack that resulted in a breach in the security of Workforce's electronic data system.

- Upon discovering that the breach occurred, Workforce immediately took steps to secure its data system, contacted law enforcement, and began an investigation into the matter with the assistance of a cybersecurity firm.

- Our investigation determined that an unauthorized party accessed Workforce's electronic data system between February 18, 2022, and March 3, 2022.

- Workforce's initial investigation revealed that certain individuals' personal data was likely accessed by the breach, and Workforce promptly notified those individuals of the breach—importantly, unless you received a previous notification from Workforce, you were not among those individuals.

- However, the investigation also suggested that additional personal data may have been included in the breach, but the initial investigation could not show which additional individuals may have been affected by the breach nor what personal data may have been included in the breach. In order to determine whether or not additional individuals' personal data was included in the breach, Workforce devoted significant staff-time and resources, engaged additional data security professionals, and spent several months conducting a broader analysis of the breach.

- Unfortunately, Workforce was unable to determine with specificity whether or not additional individuals' data was included in the breach, including yours.

- Therefore, out of an abundance of caution, Workforce is notifying all of its clients, including you, of the breach, in case your personal information may have been accessed by the breach. To date, Workforce's investigation has not revealed that your data was included in the breach or any evidence of actual or attempted misuse of your information as a result of this incident.

What Information Was Involved? The breach involved computerized data that potentially includes personal information. Such personal information potentially includes but is not limited to personal information you may have submitted to Workforce, such as driver's license number, state identification card number, or social security number.

What We Are Doing. In response to this incident, Workforce has implemented various enhanced security protocols. We are working with third-party specialists to further secure our network, and we are updating our policies and procedures related to data protection.

What You Can Do. We encourage you to remain vigilant by reviewing your various account statements and credit reports for any unauthorized activity. For more information on enrolling in free identity protection services, including some additional steps you can take to help protect your information, please see the document titled "Additional Steps You Can Take" enclosed with this notice.

For More Information. We understand that you may have questions about this notice or the incident. If so, please feel free to call us at 888-562-7571 or write us at 2125 Kern Street, Suite 208, Fresno CA 93721.

Sincerely,
Blake Konczal
Executive Director

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.
After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.