DISTRICT OFFICE:
P.O. Box 222700
Carmel CA 93922

4380 Carmel Valley Road
Carmel, CA 93923

TEL: (831) 624-1546
FAX: (831) 624-1726
www.carmelunified.org

«AddressBlock»

March 8, 2019

By U.S. Mail

Notice of Data Breach

RE: «Employee_Last_First»; «Spouse_Name»; «Dependent_1»; «Dependent_2»; «Dependent_3»; «Dependent_4»

«GreetingLine»

We are writing to notify you of a potential security incident that may have involved certain personal information you (or a spouse or parent who is an employee) provided to the Carmel Unified School District ("District"). We are providing this notice as a precaution to inform potentially affected individuals about the incident and to call your attention to some steps you can take to help protect yourself. We sincerely regret any concern this may cause you.

What Happened?

We recently learned that an outside individual sent a "phishing" email to certain District employees that resulted in unauthorized access to some District employees' email accounts. One of those accounts contained a limited number of documents that included certain personal information. While the District does not have any way to determine whether or not any particular information within the account was accessed, we are providing notice to all individuals whose information was stored in the account out of an abundance of caution.

What Information Was Involved?

The information stored in the affected email account varies by individual, but may include:

- Employee social security numbers
- Spouses' and dependents' social security numbers
- Employee/spouse marriage certificates
- Employee dependents' birth certificates
- Doctor's notes excusing employees from work or authorizing them to return to work, some with sensitive medical information

Based on our investigation, it appears you were one of the individuals whose information was stored in the account and therefore your information could be affected by this incident. Our investigation has not found any evidence that this incident involves any unauthorized access to or use of any of the District's

internal computer systems or network. Please note, at this time, we are not aware of any fraud or misuse of your information as a result of this incident.

What We Are Doing.

We take the privacy of personal information seriously and deeply regret that this incident occurred. The District has already taken the following steps in response to this incident:

- Identified the "phishing" message characteristics and removed all known copies of the message from users' mailboxes.
- Adjusted our mail system settings to enhance detection for this message or similar "phishing" messages, as well as providing a visual warning to users for suspicious messages.
- Sent initial and follow up notices to employees about this incident by phone, text, and email.
- Reset all employee passwords.

The District is currently taking these additional steps:

- Working closely with the Monterey County Office of Education to improve data security and ensure the confidentiality of your personal information.
- Auditing its practices of document transfer, email storage, and encryption.
- Reviewing current computer security training practices and developing more cybersecurity training for employees.

To help protect your identity, we are offering one year of complimentary identity protection services from a leading identity monitoring services company. These services help detect possible misuse of your personal information and provide you with superior identity protection support focused on immediate identification and resolution of identity theft. For more information about these services and instructions on completing the enrollment process, please refer to the enrollment instructions included with this letter.

What You Can Do.

On January 9, 2019, the District sent employees an initial notice of this incident, prompting them to enable two-step authentication for their Gmail accounts, change passwords for any accounts linked to their District account or that share the same credentials as their District account, and notify the District if they have provided their username or password in response to the "phishing" email. We urge employees to take these steps in order to help prevent this type of incident from reoccurring in the future.

Although we are not aware of any misuse of any information arising out of this incident, we want to make you aware of steps that you can take as a precaution:

- **Activating the Complimentary Identity Protection Services.** As outlined above, we are offering one year of identity theft protection and credit monitoring services at no charge to you. For more information about these services and instructions on completing the enrollment process, please refer to the "Information about Identity Theft Protection" reference guide attached to this letter. Note that you must complete the enrollment process by **June 30, 2019.**

- **Checking Credit Reports and Financial Accounts.** You can carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything

you do not understand, call the credit agency immediately. If you find any suspicious activity on your credit reports, call your local police or sheriff's office, and file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records. You can also review your financial account statements to determine if there are any discrepancies or unusual activity listed. If you see anything you do not understand, call the financial institution immediately.

- **Reviewing Explanation of Benefits Documents.** You can also review explanation of benefits statements that you receive from your health insurer or health plan or review for persons whose medical bills you assist with or pay (such as your child). If you identify services listed on the explanation of benefits that were not received, please immediately contact your insurer or health plan. You may also want to request a copy of your medical records from MCSIG. For more information regarding your medical privacy rights, you may visit the website of the California Office of Privacy Protection at www.privacy.ca.gov.

- **Consulting the Identity Theft Protection Guide.** Finally, please review the "Information about Identity Theft Protection" reference guide, included here, which describes additional steps that you may wish to take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on placing a fraud alert or a security freeze on your credit file.

For More Information.

Please keep a copy of this notice for your records. We take the security of your information very seriously, and we truly regret any inconvenience this incident may cause you. If you have any questions or concerns, please do not hesitate to contact Anna Medina at the District Office at (831) 624-1546 ext. 2041, and she will direct your question to the right person.

Sincerely,

Paul Behan
Chief Technology Officer
Carmel Unified School District

Rob Perry
Network Administrator
Carmel Unified School District

Information about Identity Theft Protection

Identity Theft Protection Guide

To help protect your identity, we are offering a complimentary membership in Experian's® *IdentityWorks*®. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft. Included with this service are fraud resolution services that provide an Experian Fraud Resolution agent to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition). While this Fraud Resolution assistance is immediately available to you without any further action on your part, you can also activate the fraud detection tools available through enrolling in *IdentityWorks*® at no cost to you.

To enroll in these services, visit: **www.experianidworks.com/3bcredit** by June 30**, 2019**, and use the following activation code(s) for each person that was potentially affected:

«Employee_Experian_Code» Assigned to: «Employee_Last_First»

«Spouse_Experian_Code» Assigned to: «Spouse_Name»

«Dependent_1_Experian_Code» Assigned to: «Dependent_1»

«Dependent_2_Experian_Code» Assigned to: «Dependent_2»

«Dependent_3_Experian_Code» Assigned to: «Dependent_3»

«Dependent_4_Experian_Code» Assigned to: «Dependent_4»

You may also enroll over the phone by calling **877-890-9332** between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **[ENGAGEMENT].**

Once you enroll in *IdentityWorks*, you will have access to the following features:

- **Experian credit report at signup:** See what information is associated with your credit file.
- **Active Surveillance Alerts:** Monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Fraud Resolution:** Identity Theft Resolution agents are immediately available to help you address credit and non-credit related fraud.
- **ExtendCARE**: You receive the same high-level of Fraud Resolution support even after your *IdentityWorks* membership has expired.

- **$1 Million Identity Theft Insurance[1]:** Provides coverage for certain costs and unauthorized electronic fund transfers

There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information.

Review Accounts and Credit Reports: You can regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed at the bottom of this page.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Information About Medical Identity Theft: Patients who pay for medical services can regularly review the explanation of benefits (EOB) statements that they receive from their health insurers or health plans. If they identify services listed on the EOB that were not received, they should immediately contact the health plan. For more information about protecting yourself from the Department of Health and Human Services, please visit https://oig.hhs.gov/fraud/medical-id-theft.

Security Freezes and Fraud Alerts: You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

---

[1] Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

National Credit Reporting Agencies Contact Information

Equifax (www.equifax.com)
General Contact:
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts and Security Freezes:
P.O. Box 740256, Atlanta, GA 30374

Experian
(www.experian.com)
General Contact:
P.O. Box 2002, Allen, TX 75013
888-397-3742

Fraud Alerts and Security Freezes:
P.O. Box 9556, Allen, TX 75013

TransUnion
(www.transunion.com)
General Contact, Fraud Alerts and Security Freezes:
P.O. Box 2000
Chester, PA 19022
888-909-8872