San Diego Unified
SCHOOL DISTRICT

EUGENE BRUCKER EDUCATION CENTER
4100 Normal Street
San Diego, CA 92103-2682
Phone: (619) 725-8000
Fax: (619) 725-7105

December 21, 2018

Dear San Diego Unified families:

Notice of Data Breach

This letter is in regard to an incident at San Diego Unified School District involving the security of you or your student's personal data on the district's information systems. We sincerely regret to inform you that, after completing a thorough forensics investigation, we have reason to believe your personal data may have been compromised through the access or use by an unauthorized individual. The unauthorized access resulted in the potential viewing or theft of the personal data of some students and staff members. The personal data potentially included social security numbers and other information listed below. The San Diego Unified School District has taken the steps necessary to eliminate the threat to your personal data and implement improvements to prevent such unauthorized access from happening again. We are sending this letter to provide you more information about the incident and what you can do to remain vigilant and protect your information.

What Happened

During October 2018, Information Technology professionals were investigating multiple reports of phishing emails, which were used to gather log-in information of staff members throughout the district. Staff determined an unauthorized person or persons, was gathering network access log-in information from staff and using that information to log into the district's network services, including the district student database. Access to the student database offers complete access to personal identifying information, potential health information, scheduling and grade information. All staff members whose accounts were compromised had the security on their accounts reset immediately upon discovery. The breach is believed to date back to January 2018.

What Information Was Involved

The accessed systems contained the following personal information:

- Student and selected staff personal identifying information, to include: first and last name, date of birth, mailing address, home address, telephone number;
- Student enrollment information, to include: schedule, discipline incident information, health information, school(s) of attendance, transfer information, legal notices on file, attendance data;
- Student and selected staff Social Security Number and/or State Student ID Number

- Student and staff parent, guardian and emergency contact personal identifying information, to include: first and last name, phone numbers, address (if provided), email address, employer information;
- Selected staff benefits information, to include: health benefits enrollment information, beneficiary identify information, dependent identity information, savings or flexible spending account information;
- Selected staff payroll and compensation information, to include: viewable paychecks and pay advices, deduction information, tax information, direct deposit financial institution name, routing number and account number, salary and leave information;

Access to the systems noted also included the ability to alter data within those systems.

We are not able to confirm, specifically, whether your personal data was viewed or copied from our systems as a result of this incident. We only know that the viewing or copying of some personal data was possible or occurred between January 2018 and November 1, 2018.

What We Are Doing

Once aware of the threat to student and staff data, we promptly took steps to secure the system and identify the scope of the incident with the help of law enforcement. We have continued to implement and explore additional security measures, and continue to review and audit our practices to prevent this from happening again. We have also coordinated our investigation and response to the incident with law enforcement to bring the perpetrator(s) of this incident to justice. We have also provided notice of this incident to state authorities as required under applicable state laws.

What You Can Do

We highly recommend you review all credit information for all persons listed in the student or staff databases. Remain vigilant and report any fraudulent activity to your card-issuing bank, card issuer, or credit reporting agency as soon as possible. Regardless of whether or not you note any fraudulent activity on your card statement, we still recommend that you contact credit reporting agencies to notify them of the breach of your information.

Should you find evidence of identity theft, you can contact San Diego Unified School Police Department to file a police report. To file a police report, contact your local Campus Police Officer, or call School Police Dispatch at (619) 291-7678. San Diego Unified School District Police Department is tracking all incidents of crime related to this network intrusion, and is investigating with the assistance of forensic computer and electronic crimes investigators. You may also contact the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

For More Information:

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 reporting agencies at one of the phone numbers listed below or visiting their respective websites. Some states may charge a fee for such services.

Equifax - 1-888-766-0008
P.O. Box 740256 Atlanta, GA 30348
www.equifax.com

Experian - 1-888-397-3742
P.O. Box 4500 Allen, TX 75013
www.experian.com

TransUnion - 1-800-680-7289
P.O. Box 2000 Chester, PA 19022
www.transunion.com

Under state law, a security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. To place a security, freeze on your credit report, you must send a written request to each of the three major credit reporting agencies listed above. The credit reporting agencies may also allow you to request such a security freeze online.
In order to request a security freeze, you will need to provide the following information:
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, provide the addresses where you have lived over the prior five years;
5. Proof of current address such as a current utility bill or telephone bill;
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. 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.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you 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. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

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 may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC by using the information below.
Federal Trade Commission 1-202-326-2222
Bureau of Consumer Protection 600 Pennsylvania Avenue, NW Washington, DC 20580

Additional information to help protect your privacy and identify can be located at the California Attorney General's website at the following link: https://oag.ca.gov/idtheft/information-sheets

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at (619) 260-5476, or go to: **www.sandiegounified.org/datasafety**

Sincerely,

Toren Allen
Executive Director
Integrated Technology