May ___, 2017

Name
Address
City, State, Zip

NOTICE OF DATA BREACH

Dear ____________________:

The confidentiality of the personally identifiable student information we maintain is critically important to Mt. Diablo Unified School District ("District") and we take great efforts to protect it. Regrettably, we are writing to let you know about an incident involving some of that information.

What Happened?

On April 27, 2017, when parents tried to access their student's data through the HomeLink Portal, they were able to view information, as described below, of a student other than their own. The period of time parents and students had inadvertent exposure to another student's information was one hour—between 8:00 p.m. and 9:00 p.m. and the data of approximately 600 families was exposed. The District has no reason to believe that any personally identifiable student information was accessed by an unauthorized person; however, it was possible during this brief window. Once the District learned of the problem, we immediately took HomeLink offline and began working with our Student Information System provider ("Eagle Soft") and with Microsoft. Eagle Soft and Microsoft have identified the malfunction as a caching problem that has now been repaired. Please note that the District is operating HomeLink as intended by Eagle Soft and Microsoft. The error occurred due to a software malfunction that was outside of the District's control.

What Information Was Involved?

The information that was accessible during the one-hour timeframe of inadvertent access was: address; home phone numbers; immunization records; required medication; medical history; grades; class schedules; test scores; parent email addresses; attendance; and transcripts.

What We Are Doing

We have no reason to expect this will happen again and there is no evidence the inadvertently accessible information has been improperly used. However, out of an abundance of caution, we have also notified law enforcement. We have also reported the breach to the California Office of the Attorney General. In order to minimize the risk of future malfunctions, we have reviewed our existing procedures and Microsoft and Eagle Soft are conducting an audit of their software to identify any vulnerability.

What Can You Do

Neither financial information nor social security numbers were accessible. However, if you are concerned about identity theft, you should monitor your credit card account for suspicious transactions and report any to the card-issuing bank. You can also ask your bank for online monitoring and alerts on the card account. This will give you early warning of any fraudulent transactions.

No insurance information or medical plan numbers were accessible during the above-referenced breach. However, it's a good idea to watch the Explanation of Benefits statements of any insurance notification you receive for any questionable items. If you see a service that you did not receive, follow up on it with your insurer or plan. For more on medical identity theft, see "First Aid for Medical Identity Theft: Tips for Consumers", at www.oag.ca.gov/privacy/info-sheets.

For More Information

For more details on what to do if you suspect that your information is being used to commit identity theft, see the Identity Theft Victim Checklist at www.oag.ca.gov/idtheft/information-sheets. We sincerely apologize for the concern and inconvenience this situation may cause you. If you have any questions, please do not hesitate to contact Ursula Leimbach at____________.

Sincerely,

____
[Title]