April 17, 2017

Dear current or former student,

Palo Alto Unified School District (PAUSD) was contacted late last week by a former vendor, Schoolzilla, informing the school district that there had been unauthorized access to its network and data. Schoolzilla is the data warehouse vendor that PAUSD contracted with from May 2015 to May 2016 for data reporting services. PAUSD's contract with Schoolzilla ended in May 2016. As directed by California law, families of identified students are being notified by US Mail.

What happened?

After a recent upgrade to their backup systems, a configuration error exposed Schoolzilla's backup files. A computer security researcher doing targeted vulnerability analysis detected this issue late on April 4, 2017, downloaded those files, and notified Schoolzilla of the problem. As soon as Schoolzilla received the notice on the morning of April 5, 2017, they immediately fixed the error, verified via log files that nobody other than the one security researcher accessed those exposed files, and ensured that the security researcher who discovered and alerted us to this vulnerability permanently and securely deleted the data.

What information was involved?

We have been informed that the researcher was able to access an off-site backup that included partial student records for approximately 14,000 of our students. This information includes names, addresses, birth dates, and test scores from historic CAASPP, CAHSEE, and CELDT state assessments. The data also included parent names, though there was no additional parental information present in the files. The breach **did not** include other personal information about the student or family such as Social Security or Driver's License numbers, email addresses, or any passwords associated with PAUSD services. PAUSD does not have electronic records of student or parent/guardian Social Security numbers, Driver's license numbers, or California identification card numbers. At this time, the security vulnerability has been fixed and Schoolzilla logs indicate no other access to the data. The researcher has provided a sworn affidavit to Schoolzilla stating that all data from the incident has been deleted.

What are we doing?

The privacy of your personal information is of the utmost importance to PAUSD. While the initial review of current contracts show we are in compliance with California Education Code §49073.1, we are continuing to dialog with our vendors regarding the implementation of safeguards to protect your personal information. Pursuant to California Information Practices Act of 1977 (Civ. Code §1798), this incident will be reported to the California Attorney General for further investigation. In addition, we have contacted the US Department of Education's Privacy Technical Assistance Center for further guidance with this incident.

What can you do?

PAUSD and Schoolzilla are available to speak with you and provide any additional information. Please contact either organization if you have questions (contact information is below). Also, the researcher affirmed and swore under penalty of perjury that he deleted all the records and does not know which school districts' data he had obtained in his process of confirming the vulnerability.

While this situation is undesirable and unfortunate, it is an opportunity to remind ourselves about important steps we can take to protect our personal data every day. Consider a family plan for digital privacy and protection and talk to your children about these important issues.

For more information:

We will continue to be in regular contact with the vendor and would be happy to answer any further questions: Christopher Kolar, Director of Research and Assessment ckolar@pausd.org, or Derek Moore, Chief Technology Officer dmoore@pausd.org. More information is available on the Schoolzilla blog or by email: security@schoolzilla.com.