

ETS Incident Facts for Front Office Staff /School Leaders

- The California Department of Education has informed school districts about a data security incident involving Educational Testing Service (ETS), the contractor that administers California's statewide assessments.
- This incident did not involve our school or district computer systems.
- ETS will notify you by email or mail if you or your student's information was impacted.
- In the meantime, you can go online to [CDE.CA.GOV/ETS](https://cde.ca.gov/ets) and find details and questions.
- When you're on that website you can find out how to enroll in a complimentary identity protection program that's good for two years.
- If you want to call to get more information, the number is 833-931-8488. They're open Monday through Friday from 6 a.m. to 6 p.m.

Website Content (short)/ Newsletter Blurb

The district/school was recently notified of a data security incident involving Educational Testing Service (ETS), the nonprofit contractor that provides state- and federal-required testing to all students enrolled in California public schools. You will be notified via mail or email if you or your student were impacted. ETS is offering two years of complimentary credit monitoring and identity protection services through Experian Identity Works for all affected students. For more information, visit www.cde.ca.gov/ets or call 833-931-8488.

Website Content (long) - FAQ style

The district/school was recently notified of a data security incident involving Educational Testing Service (ETS), the nonprofit contractor that provides state- and federal-required testing to all students enrolled in California public schools.

According to information provided by CDE and ETS, unauthorized access to student records was identified on Sept. 25, 2026. The incident affected data associated with California public school students enrolled during the 2023-24 school year through the current school year, regardless of whether a student participated in state testing.

What information was involved?

The compromised records may include student information such as:

- Student name and date of birth
- Home address

- School, district, and grade level
- Statewide identifier
- Student gender, ethnicity, and primary language
- English learner status, disability status, eligibility status for Title I, etc., and English language proficiency

The data did not include:

- Social Security numbers
- Driver's license numbers or passport numbers
- Financial accounts or payment cards
- Passwords
- Parent/guardian personal information (with the exception of home address)

Is my student impacted?

ETS, at the direction of CDE, is notifying affected students and families whose information was accessed and copied during the incident. If you receive a notification letter and/or email about the incident, this means your and/or your student's information was included in the files which were accessed and copied.

What can you do now?

Identify protection: As a precaution, ETS is offering two years of complimentary credit monitoring and identity protection services through Experian Identity Works for all affected students.

- For minors, enroll at: www.experianidworks.com/minorplus
- For adults, 18 and older, enroll at: www.experianidworks.com/identity

Questions and More Information: ETS has established resources to answer questions and provide additional information about the incident, including enrollment information for identity protection services.

- For answers to frequently asked questions and additional details about the incident visit: www.cde.ca.gov/ets.
- For questions about the incident, please call 833-931-8488, Monday – Friday, 6 a.m. to 6 p.m. Pacific Time. If you have a speech or hearing impairment and use a TTY, please call 711. Please provide your engagement number:
 - B174774 for students under 18
 - B174775 for students 18 or over

Our Commitment

We understand that news of a data security incident involving student information is very concerning. While this did not occur within our district's systems, this is a reminder for all of us to stay vigilant when it comes to cybersecurity. Protecting you and your student's personally identifiable information is a top priority.

[Optional: Specific steps taken at your school/district to keep student information secure or link to cybersecurity board policy.]