



[Home](#) / [Newsroom](#) / [Incident Notices](#) / [Educational Testing Service \(ETS\) Incident](#)

Educational Testing Service (ETS) Incident

Educational Testing Service (ETS), at the direction of the California Department of Education (CDE), is notifying California students and families about a data security incident involving an ETS-operated secure file transfer protocol (SFTP) site, the steps being taken to protect their information, and available resources and support.

Navigate this page:

[Notification of Data Breach Letter](#)

[Frequently Asked Questions for California Students and Families](#)

[Additional Resources and Assistance](#)

[Additional Incident Communications](#)

Notification of Data Breach Letter - Available in multiple languages

- [ETS Notification page](#)
-

Frequently Asked Questions for California Students and Families

Jump to a topic:

[What happened, and who is ETS?](#)

[What information was involved?](#)

[How will I know if my information or my child's information was accessed and copied?](#)

[Does this incident affect former students, including those who are now adults?](#)

[Who is eligible for complimentary identity-protection services, and how do I enroll?](#)

[What if I don't receive a notification letter?](#)

[What can affected individuals do to protect their information?](#)

[How can I tell whether communication about this incident is legitimate?](#)

[What are ETS and the state doing to address the incident and prevent future incidents?](#)

[Why did ETS have access to this information?](#)

1. What happened, and who is ETS?

ETS is a nonprofit assessment organization under contract with the State of California to provide state and federally required testing to all students enrolled in California public schools. ETS supports California's statewide assessment programs, including the California Assessment of Student

Performance and Progress (CAASPP) and the English Language Proficiency Assessments for California (ELPAC).

On September 25, 2026, ETS identified unauthorized activity involving a secure file transfer protocol (SFTP) site used to exchange California statewide assessment information with CDE.

ETS disabled the account involved, took the affected SFTP site offline, and initiated an investigation with external cybersecurity experts. The investigation determined that an unauthorized party used a compromised login credential to access the site and copy files containing California student information at various times between May 22 and September 18, 2026.

After working with law enforcement as well as with cybersecurity experts, ETS has taken steps to reduce the potential risk of the data being made publicly accessible.

ETS, following regular web monitoring, has, to date, not uncovered any evidence that the information has been made public.

2. What information was involved?

Information about California students, including but not limited to all students enrolled in the three previous school years, was accessed and copied. The information that was accessed and copied contained student demographic, program participation, and assessment data that ETS maintains in connection with California's statewide assessment programs.

The student information accessed and copied varies by individual, but may include:

- Student names, dates of birth, residential addresses, schools, districts, and grade levels.
- Statewide Student Identifier (SSID) and local student identifier. A Statewide Student Identifier (SSID) is a unique, randomly generated 10-digit number assigned to an individual student within the California public K-12 educational system. Learn more at www.cde.ca.gov/ds/sp/cl/ssid.asp.
- Demographic information, including gender, race or ethnicity, primary language, country of origin, and English learner status.
- Disability and Section 504 status, testing accommodations, and primary disability type.
- Eligibility status for the following programs: Title I, Part A; Title I, Part C; McKinney-Vento; and Military Connected Student.
- English language proficiency information and statewide assessment registration, participation, and results, where applicable.

Not every student's record contained all these types of information.

The data accessed and copied did not include Social Security numbers, driver's license numbers, passport numbers, financial account information, credit or debit card information, or account passwords. The incident did not involve parent or guardian personal information.

After working with law enforcement as well as with cybersecurity experts, ETS has taken steps to reduce the potential risk of the data being made publicly accessible.

ETS, following regular web monitoring, has, to date, not uncovered any evidence that the information has been made public.

3. How will I know if my information or my child's information was accessed and copied?

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 accessed and copied.

Not receiving a notification does not necessarily mean your and/or your student's information was unaffected.

Affected individuals include current and former students enrolled in California public schools between 2023 and the current school year, as well as students who left a California school since 2006 and did not confirm transfer to another school with the CDE.

The notification explains what happened, the types of information involved, what steps the State is taking, what steps ETS is taking, available identity-protection services, and steps you can take to protect personal information.

4. Does this incident affect former students, including those who are now adults?

Yes. The incident may affect former students, including but not limited to individuals who were enrolled in a California school in the three previous school years.

Affected former students, including those who are now adults, are eligible for complimentary identity-protection services if their information was accessed and copied during the incident.

5. Who is eligible for complimentary identity-protection services, and how do I enroll?

ETS is providing 24 months of Experian IdentityWorks identity-protection services to affected current and former students whose information was accessed and copied at no cost to affected individuals.

Two service packages are available:

- Minors under 18: Parents or legal guardians can enroll affected students in Experian IdentityWorks Minor Plus. The enrollment deadline for this product is on or before March 19, 2027. Visit the Experian IdentityWorks website to enroll: www.experianidworks.com/minorplus.
 - ❖ Affected minors who turn 18 before March 19, 2029 may enroll in the adult product upon turning 18 using the adult product activation code provided with the notification.
- Adults 18 and older: Affected adults, including former students, can enroll directly in Experian IdentityWorks. The enrollment deadline for this product is on or before March 19, 2027. Visit Experian IdentityWorks website to enroll: www.experianidworks.com/identity.

- Enrollment instructions, including the website and activation code, are provided with the notification [ETS Notification page](#).

Enrollment is provided at no cost to the affected individual, and no credit card is required.

Experian also provides identity restoration assistance to eligible affected individuals who experience identity theft. This assistance is available for 24 months from the date of the notification and does not require enrollment in monitoring services.

6. What if I don't receive a notification letter?

Not receiving a notification letter does not necessarily mean your information was not affected. Some current and former students may not receive a notification, particularly if their contact information has changed.

Affected individuals include current and former students enrolled in California public schools between 2023 and the current school year, as well as students who left a California school since 2006 and did not confirm transfer to another school with the CDE.

Visit [ETS Notification page](#) for information on identity-protection services, and instructions to get assistance.

7. What can affected individuals do to protect their information?

We encourage affected individuals to consider enrolling in the identity protection services and remain alert to possible misuse of student personal information.

It is always best practice to be cautious of unexpected emails, text messages, or phone calls referencing a student's school, statewide assessments, or this incident. Do not share personal information, passwords, or financial information in response to unsolicited requests. Verify website addresses before entering personal information to enroll in identity-protection services.

Adults can obtain free credit reports at www.annualcreditreport.com or by calling 1-877-322-8228. Adults may place a free security freeze on their own credit files.

Parents and guardians may also consider requesting a free credit freeze for their children who are under 16 to help prevent unauthorized accounts from being opened in their name.

For additional information about credit reports, fraud alerts, and security freezes, contact:

- Equifax: 800-685-1111 | www.equifax.com
- Experian: 888-397-3742 | www.experian.com
- TransUnion: 833-799-5355 | www.transunion.com

Although Social Security numbers and financial account information were not involved, taking precautions to protect personal information is encouraged.

8. How can I tell whether communication about this incident is legitimate?

Be cautious of unexpected emails, phone calls, or text messages claiming to be from ETS, CDE, or Experian about this incident.

Do not provide Social Security numbers, passwords, financial information, or other sensitive personal information in response to unsolicited requests.

Affected individuals will receive instructions for enrolling in complimentary identity-protection services in their notification letters [ETS Notification page](#).

Enrollment is free and does not require a credit card.

If you are unsure whether a communication is legitimate, visit CDE's official incident webpage at www.cde.ca.gov/ets for information.

9. What are ETS and the state doing to address the incident and prevent future incidents?

Following discovery of the incident, ETS has taken numerous measures to enhance the security of the SFTP site, including taking the SFTP site offline and building an entirely new SFTP site with enhanced security controls. ETS continues to evaluate additional security measures that may be appropriate.

After working with law enforcement as well as with cybersecurity experts, ETS has taken steps to reduce the potential risk of the data being made publicly accessible. Furthermore, ETS, following regular web monitoring, has, to date, not uncovered any evidence that the information has been made public.

CDE and the State Board of Education (SBE) are working with state cybersecurity experts to assess the incident's impact on California students and families and ensure affected individuals receive appropriate information and support.

The California Cybersecurity Integration Center (Cal-CSIC) is assisting with digital forensics and incident response. The California Department of Technology (CDT) and California Governor's Office of Emergency Services (Cal OES) are also supporting the state's technical, legal, and operational response.

CDE and SBE are reviewing the incident and ETS's compliance with applicable data security and contractual requirements.

10. Why did ETS have access to this information?

ETS is a nonprofit assessment organization under contract with the State of California to provide state and federally required testing to all students enrolled in California public schools.

ETS maintains student demographic, program participation, and assessment data in connection with California's statewide assessment programs.

Additional Resources and Assistance

- Notification letters in multiple languages: [ETS Notification page](#)
- Experian identity-protection services enrollment:
 - ◆ For minors, visit the Experian IdentityWorks website to enroll:
www.experianidworks.com/minorplus
 - ◆ For adults, 18 and older, visit Experian IdentityWorks website to enroll:
www.experianidworks.com/identity
- Questions about the incident, please call 833-931-8488, Monday – Friday, 6:00 am to 6:00 pm 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
- Identity-theft prevention resources: California Department of Justice, www.oag.ca.gov/privacy
- For media inquiries, please submit your request through CDE's [Media Inquiry Form](#).

Additional Incident Communications

- [Updated Procedures for English Learner Inclusion in Unduplicated Pupil Count Letter](#)
- [Educational Testing Service \(ETS\) Letter](#)

This webpage will be updated as additional information becomes available.

Questions: 833-931-8488

Last Reviewed: Friday, October 16, 2026