

TO: Chief Executive Officers
Chief Student Services Officers
Chief Information Systems Officers
Chief Instructional Officers
Chief Business Officers
Admissions and Records Officers
Financial Aid Officers

FROM: Chris Ferguson, Executive Vice Chancellor, Finance and Strategic Initiatives
Jory Hadsell, Executive in Residence, Strategic Technology Initiatives
Craig Hayward, Vice Chancellor of AI Strategy and Digital Transformation

RE: Implementation of Required Digital Identity Verification

Purpose

The California Community Colleges Chancellor's Office continues to advance systemwide measures to protect students, preserve access to educational opportunity, strengthen the integrity of admissions and enrollment processes, and reduce the impact of application, enrollment, and financial aid fraud across the system.

This memorandum provides guidance for the next phase of the Chancellor's Office's ongoing fraud mitigation strategy and informs the movement away from opt-in identity verification to required digital identity verification, effective August 11, 2026.

Beginning August 11, 2026, applicants for admission to the California Community Colleges system will be required to have their identity verified through an approved online process or via local in-person verification steps before an application for admission is delivered to a college Student Information System (SIS) from the statewide admission portal (CCCApply or CCCStart). Verification may occur through a student-facing digital verification prompt, secure pathway-based data sharing, a special admission process, or local in-person verification when needed.

Additional technical guidance, frequently asked questions, and implementation resources will be provided by the CCC Technology Center and the Chancellor's Office through a forthcoming Digital Identity Verification Toolkit, detailed later in this memorandum.

Background and Ongoing Fraud Elimination Efforts

Since 2020, the California Community Colleges system has experienced increasingly sophisticated fraud activity affecting admissions, enrollment, and financial aid processes. Prior Chancellor's

July 23, 2026

Office guidance has distinguished among admission application fraud, enrollment fraud, and financial aid fraud because each occurs at a different point in the student journey and requires coordination among systemwide technology services, local college processes, student services, admissions and records, financial aid, faculty, and information technology teams.

The Chancellor's Office, in partnership with the CCC Technology Center and local colleges and districts, has implemented multiple layers of fraud mitigation and identity protection over time, including enhancements to OpenCCC, CCCApply, multi-factor authentication, spam and bot detection, ID.me identity verification, the California DMV Mobile Wallet, and AI-enabled fraud detection tools. These efforts build upon prior Chancellor's Office communications and guidance, including:

1. DII 21-200-02, *Admission Application Fraud and Financial Aid Fraud*, dated June 22, 2021;
2. ESS-21-300-013 *Mitigating Enrollment Fraud - Instructional Practices & Reporting Obligations*, dated September 20, 2021;
3. DII 23-200-05, *Important Update: Pilot Integration of Identity Proofing into CCCApply*, dated November 14, 2023;
4. ISTI 25-200-01, *Deployment of California Department of Motor Vehicles (DMV) Mobile Wallet as Additional Identity Verification Option within OpenCCC and CCC Apply*, dated November 7, 2025.

The August 11, 2026 implementation of required digital identity verification is the next phase in evolving and further strengthening systemwide protections, moving the system from an opt-in verification model to a standardized methodology for securely authenticating real students across the California Community Colleges. The goal is not simply to check a document at a single point in time, but to establish trusted digital identity signals that protect real students, reduce fraud, and support secure movement through admissions, enrollment, and financial aid processes.

Student Access, Privacy, and Equity

The transition from an opt-in model to required digital identity verification is intended to protect real students, safeguard financial aid and class availability, and preserve the integrity of public resources. It is not intended to discourage or prevent eligible students from applying to a California community college.

The Chancellor's Office will continue to work with system partners to ensure that verification options are accessible to California's diverse student populations, including students who may use different forms of identity documentation, adult learners, returning students, students with disabilities, students with limited access to technology, and minors participating in dual enrollment or other early college pathways.

For domestic applicants, digital identity verification is intended to authenticate identity, not to determine immigration or citizenship status. The California Community Colleges do not collect or store information regarding citizenship. Information needed for international student admission will continue to be handled through the appropriate international student application pathway.

All digital identity verification processes must continue to comply with applicable federal and state privacy, accessibility, and student records requirements.

System Standard and Guiding Frameworks

The Chancellor's Office is establishing a systemwide digital identity verification standard as part of its continued layered approach to fraud mitigation, student identity protection, data integrity, and responsible stewardship of public resources.

Where student-facing digital identity proofing is used through approved verification providers, the Chancellor's Office is aligning those methods to National Institute of Standards and Technology (NIST) Special Publication 800-63 Digital Identity Guidelines, including Identity Assurance Level 2 (IAL2).

The IAL2 standard establishes a higher level of confidence in a claimed identity by requiring stronger evidence, validation, and verification than basic self-asserted identity approaches. Where necessary, the Chancellor's Office may utilize IAL2-equivalent profiles that are risk-adjusted for specific use cases (e.g., dual enrollment) as part of risk-based compliance management and ensuring student access.

The Chancellor's Office's broader approach to fraud mitigation, information security, AI-enabled detection, third-party technology integration, and risk management is also informed by prominent security and fraud-risk frameworks, including:

- NIST Cybersecurity Framework (CSF);
- NIST AI Risk Management Framework (AI RMF);
- California Digital ID Framework;
- Center for Internet Security (CIS) Critical Security Controls; and
- U.S. Government Accountability Office Framework for Managing Fraud Risks in Federal Programs.

Consistent with these standards and frameworks, the Chancellor's Office's approach includes:

- Clear systemwide standards and implementation timelines;
- Layered technical and operational controls;
- Risk-based identity verification and fraud detection;
- Protection of student privacy and institutional data;
- Monitoring, feedback, and continuous improvement; and
- Attention to equitable access for real students.

Verification Pathways and Student Experience

The Chancellor's Office will use a layered approach to digital identity verification and fraud mitigation as no single tool or method is sufficient for all student populations or fraud scenarios.

For many applicants, digital identity verification will occur through an online student-facing verification process. Currently, the DMV Mobile Wallet, utilizing the mobile driver's license or mobile identification card, and ID.me provide this functionality. For others, including minors, students participating through high school dual enrollment or special admission pathways, and other student populations, identity may be verified through data sharing among trusted organizations (such as the Community College Guidance Initiative, California Department of Education, California Student Aid Commission, etc.) or as part of a special admittance process for enrollment. Applicants who are unable to complete online verification or who require additional review or support may be routed to local or system-supported processes as appropriate.

For applicants presented with online student-facing verification, the system may provide options to complete verification either before or after filling out the admissions application. These individuals may see options such as:

- Verify Now, which allows the applicant to complete verification before continuing through the application;
- Verify Later, which allows the applicant to complete the application first and complete verification afterward.

The "Verify Later" option does not waive or bypass the verification requirement. It only affects the workflow. Applicants who choose to verify later must complete verification, or be cleared through an approved process, before the application is delivered to the college Student Information System.

When an application belonging to an individual under age 18 is flagged as suspicious or potentially fraudulent, the applicant may be notified by e-mail or text message to complete a digital verification workflow. This workflow may include parent or guardian involvement either through one of the CCC online identity verification providers or the applicant may be provided the option to verify their identity in person.

Because fraud tactics continue to evolve, this memorandum intentionally provides general implementation guidance. Additional technical details will be provided directly to colleges through appropriate secure operational channels.

Recent System Enhancements

Several recent system improvements are supporting required digital identity verification and fraud mitigation.

DMV Mobile Wallet Expanded to Support OpenCCC Account Reset

As of April 7, 2026, DMV Mobile Wallet functionality is available in production to support OpenCCC self-service account reset processes. This enhancement provides students with an additional secure method to prove their identity and regain access to their account.

Multi-factor Authentication for OpenCCC Account Login

The CCC Technology Center has concluded its pilot of requiring multi-factor authentication on OpenCCC account login. As of June 22, 2026, this method is in full production and will continue to be used as part of the system's broader account security and identity protection strategy.

Ongoing backend upgrades to OpenCCC, CCCApply, CCCStart, fraud detection tools, and identity verification services mean that students may encounter identity verification prompts on screen or via notification in different parts of the process depending on their pathway.

The Chancellor's Office and CCC Technology Center will continue to provide technical guidance to help colleges understand how these workflows operate. Verification status and source information will continue to be delivered to colleges via SuperGlue to support local processes.

Support for Students Who Need Assistance

The Chancellor's Office recognizes that some students may be unable to complete a particular automated verification method immediately or without assistance. Colleges should maintain or establish local processes to support students who require additional assistance. This may include students who:

- Do not have access to required technology;
- Experience technical difficulty with a verification tool;
- Have identity documentation that requires additional review;
- Are under age 18 and choose to verify in person with a parent or guardian; or
- Are participating through special admission pathways where automated verification or data sharing is not available.

The forthcoming toolkit will include information to support local verification processes, support workflows, student communications, and frequently asked questions.

Students who need assistance will also be directed to available online support resources, including ccchelp.info and embedded help prompts within the student journey. Colleges may provide additional local support.

The Chancellor's Office remains committed to ensuring that fraud mitigation practices protect students and colleges without creating unnecessary barriers for legitimate applicants.

College and District Responsibilities

Colleges and districts should begin preparing now for the August 11, 2026 implementation date and should use forthcoming CCC Technology Center and Chancellor's Office resources to review and update local procedures.

1. Review local procedures for using digital identity verification information

Colleges should review procedures across admissions and records, financial aid, student services, dual enrollment, and other relevant functions to begin aligning local processes with digital identity verification information available through OpenCCC and delivered to colleges through SuperGlue. Colleges should also identify use cases where manual identity review may still be needed and develop clear information for students who require support.

2. Utilize the forthcoming toolkit and technical guidance resources

Colleges should use the Digital Identity Verification Toolkit, FAQs, sample messages, release notes, and technical guidance that will be provided by the CCC Technology Center and Chancellor's Office to:

- a.** Prepare to expand communications and support materials as the system transitions from opt-in identity verification to required verification for all applicants. Sample language and student-facing materials will be included in the forthcoming toolkit;
- b.** Identify use cases where manual identity review may still be needed and develop clear information for students who require support;
- c.** Ensure local operating procedures are in place to support applicants who do not verify or cannot verify successfully online; and
- d.** Review procedures across admissions and records, financial aid, student services, dual enrollment, and other relevant functions to align local processes with digital identity verification information available through OpenCCC and delivered to colleges through SuperGlue.

3. Continue timely monthly fraud reporting

Colleges and districts should continue submitting monthly fraud reports as a condition of receiving Local and Systemwide Technology and Data Security (LSTADS) funds. Districts should ensure that a designated college or district individual is responsible for timely submission of required monthly fraud reports.

4. Provide feedback during implementation

Colleges should provide feedback regarding student experience, staff workflows, local verification needs, and any equity or access concerns that emerge during implementation.

5. Comply with financial aid verification, recovery, and reporting practices

Colleges and districts should remain current on applicable federal and state financial aid verification and disbursement requirements. Additionally, colleges should:

- a.** Exercise due diligence and use available system intelligence before awarding aid funds;
- b.** Take appropriate steps to recover financial aid funds when fraud is later identified; and
- c.** Report financial aid fraud cases to the appropriate authorities consistent with federal and state law, regulation, and guidance.

Relationship to Reimagine CCCApply and CCCStart

The transition to CCCStart through the Reimagine CCCApply initiative represents the next evolution of the system's robust and integrated approach to admissions modernization, digital identity verification, fraud mitigation, and student experience.

CCCStart is designed to provide a modern, mobile-first, student-centered application experience while strengthening the system's ability to support digital identity verification, fraud detection, consolidated application data, and integrated college workflows. The Reimagine Apply Task Force specifically identified the need to balance equity, improved user experience, and protection against fraud in the target-state application design. (See RAD 25-01, *Reimagine Apply Task Force – March 2025*, dated March 12, 2025.)

As CCCStart is implemented, colleges will have improved visibility into application status, fraud-related information, communications, and workflow actions through more integrated platform capabilities. This approach is intended to bring together fragmented processes, reduce manual effort associated with identifying and resolving fraud and identity issues, improve the admission experience for students, and better support college staff through a more unified operational view. Additionally, all colleges using CCCStart will gain access to Socure for identity verification and Lightleap AI to detect and mitigate fraud within and across colleges and districts.

The Chancellor's Office will continue to align digital identity verification guidance with Reimagine CCCApply (CCCStart) implementation activities, CCC Technology Center release notes, and local college readiness planning. Districts are encouraged to plan and prioritize CCCStart implementation by joining one of the implementation waves during the 2026-27 year. More information and an interest form for future waves is available on the [Reimagine Apply website](#). The target date for system wide cutover to CCCStart and decommissioning CCCApply is June 30, 2027.

Forthcoming Resources and Continuous Improvement

The CCC Technology Center and Chancellor's Office will provide additional resources to support implementation, distributed through secure channels as appropriate, including:

- Digital Identity Verification Toolkit;
- Frequently Asked Questions;
- Student-facing communication templates;
- College staff guidance;
- Technical documentation;
- Release notes;
- Webinar and training materials;
- Information regarding verification status values and data availability;
- Secure forum for sharing fraud updates and effective local practices that can be shared with other districts; and
- Guidance for local verification and student support workflows.

The Chancellor's Office and CCC Technology Center will gather feedback from colleges and students during Summer 2026 and on an ongoing basis. This feedback will be used to refine student-facing messaging, technical workflows, verification status reporting, local review and exception processes, toolkit materials, and future integration with CCCStart and related systemwide platforms.

Additional information will be shared through CCC Technology Center communications, Chancellor's Office updates, and stakeholder briefings.

Questions

For policy or implementation questions, please contact:

Chancellor's Office

- Jory Hadsell, Executive in Residence for Strategic Technology Initiatives – jhadsell@cccco.edu
- Craig Hayward, Vice Chancellor of AI Strategy and Digital Transformation – chayward@cccco.edu

July 23, 2026

- Chris Ferguson, Executive Vice Chancellor, Finance and Strategic Initiatives – chris.ferguson@cccco.edu

For technical questions, please contact:

CCC Technology Center

- College Experience Managers - cems@ccctechcenter.org
- For general college staff support: staffsupportccctc@openccc.zendesk.com

cc: Sonya Christian, Chancellor
Rowena Tomaneng, Deputy Chancellor
Allison Beer, Dean, Educational Services and Support
James Todd, Vice Chancellor of Academic Affairs
Jennifer Coleman, CCC Technology Center
Reimagine CCCApply Implementation Advisory Group
Reimagine CCCApply Steering Committee