California Community Colleges

MEMORANDUM
January 31, 2022

DII 22-200-01 | Via Email

TO: Chief Executive Officers
Chief Information Systems Officers
Chief Student Services Officers
Chief Financial Aid Officers

FROM: Dr. Valerie Lundy-Wagner, Vice Chancellor, Digital Innovation and Infrastructure
RE: 2022 System Fraud Mitigation Updates

This memo describes the Chancellor's Office strategy to mitigate fraud, including partnership with the California Community College Technology Center (Tech Center), colleges and districts, and others at the state and national levels. As observed nationwide, the pandemic-induced shift to more remote engagement emboldened bad actors to target a variety of industries, including higher education and the California Community College (CCC) system specifically. This memo briefly summarizes past efforts and provides a roadmap for fraud mitigation that the Chancellor's Office will continue to evolve while remaining steadfast to prioritize real students' equitable access to an affordable postsecondary education in California.

ACTION REQUIRED: By the 10th of each month, all colleges and districts should report information on the type and scope of suspected fraud in the previous month. Details provided below.

Identifying and Characterizing Fraud

In 2021, the Chancellor's Office and Tech Center teams responded to college, district, state and federal concerns related to fraud with deeper investigation. As a first step to understand and address those challenges, the Chancellor's Office developed a typology of fraud. Three categories of fraud were eventually defined as part of a sequence where admission application fraud must first be committed before enrollment fraud can take place. Further, enrollment fraud must occur to commit financial aid fraud.

The typology has enabled stakeholders – e.g., staff in information technology (IT), institutional

research, planning and effectiveness (IRPE), admissions and records, financial aid, as well as counseling and classroom faculty – to better recognize suspicious activity and vulnerabilities. This work catalyzed a thorough review of system- and local-level processes associated with admission application, enrollment and financial aid-related fraud (as noted in the following memos, DII 21-200-02 and DII 21-200-03).

The Chancellor's Office is optimistic about the cross-divisional/unit engagement that is occurring at many colleges and how it is catalyzing the enhancement of local security processes. Given that much of the local fraud mitigation work to-date has been manual, feedback is being used to inform Chancellor's Office planning for system-level strategy including review of security technology adoption, monitoring processes, local-level infrastructure and capacity needs, and relevant policy reviews. The Chancellor's Office anticipates that system-level adjustments, once fully implemented, will meaningfully reduce the level of effort for college administrators, staff, and faculty.

Systemwide Security Infrastructure Priorities

Based on partnership with the Tech Center, the Chancellor's Office has initiated several actions to mitigate fraud in the CCC system. The following key strategies are currently underway:

- First, the Student Success Suite (i.e., OpenCCC/CCCApply/MyPath) was updated this month to include multi-factor verification of student email and/or phone number will strengthen triaging efforts with regard to admission application fraud.

- Second, the Chancellor's Office has already invested in systemwide technology infrastructure designed for colleges to share information with the Tech Center, SuperGlue. To date, it has been used for uni-directional information flows – from the Tech Center to colleges, despite the fact that the capability exists for colleges to share information back. By enabling bi-directional use of SuperGlue, whenever a college suspects or identifies admission application, enrollment or financial aid fraud, information about that application can be shared with the Tech Center, which in turn can suspend or block the profile effectively protecting all other colleges automatically. The Chancellor's Office is

planning for this functionality to be enabled by fall 2022. As relevant, colleges will be provided guidance on technical requirements needed to ensure sustainable and equitable implementation.

In the meantime, colleges should continue to make use of CCC Apply's fraud filter technology to update all applications that were not flagged as fraudulent as fraudulent when associated with a fraudulent application, as documented in DII 21-200-02.Colleges should contact: staffsupportcctc@opencc.zendesk.com to obtain assistance on the implementation of SuperGlue if it is not already deployed locally and also to report batches of fraudulent applications/profiles.

- Additionally, the Tech Center is working to further augment the security of CCCApply by adding additional data-driven fraud mitigation tools that will further enhance the ability to identify fraud at the time of application. This deployment, in addition to consistent proactive engagement with the CCCApply fraud filter (noted above), will help further improve automated processes for successfully characterizing fraudulent activity in ways that benefit the entire system. The Chancellor's Office is anticipating that this enhancement will be implemented systemwide by end of summer 2022.

- Finally, in continued conferral with other state agencies and higher education systems, the Chancellor's Office continues to investigate additional anti-fraud measures to be implemented in the future, including Identity Proofing and Identity and Access Management (IAM) technologies. For more information on Identity Proofing and IAM, please contact Stephen Heath, Information Security Consultant at sheath@cccco.edu.

More information and updates on these system-level improvements will be provided in future memoranda. All security-related decisions remain grounded in the system's commitment to digital equity for community colleges and their students.

Local Technology Infrastructure Guidance

While system-level efforts are underway to support all 116 colleges and 73 districts, college and district staff should take all steps to optimize efforts associated with local fraud mitigation. Based on information from the Tech Center, a significant number of colleges are implementing Microsoft, Google or other products which may include a multi-factor authentication (MFA) feature. All colleges and districts are encouraged to activate MFA for remote access if they have not done so already. MFA considerably reduces the risk of fraud committed through the compromise of current and former student accounts, and provides additional protection against ransomware and other cybersecurity threats.

The Chancellor's Office also recommends that all colleges develop anti-fraud automatic flagging measures. A central dashboard that collects information from multiple data sources (e.g., CCCApply, Canvas, and the local student information system, etc.) can provide local college faculty and staff with indicators that are expected to ultimately reduce faculty and staff time spent on fraud identification and reduction activities.

Reporting of Fraudulent Activity

Starting in September 2021, the Chancellor's Office requested that all colleges report monthly to provide information on the type and scope of suspected fraud across the system. Collecting these data is critical to helping the Chancellor's Office and Tech Center understand which types of fraud are occurring, take steps to remediate or block affected student accounts, provide institutional support as needed, and ensure that other colleges benefit from lessons learned.

To date, the Chancellor's Office has observed modest participation from colleges and districts in the monthly reporting of fraudulent activity. Monthly reporting of fraudulent activity is crucial to measuring the success of any anti-fraud efforts but also supports proactive systemwide efforts. Reporting each month should be submitted by the 10th of the subsequent month. Current as well as prior months can be submitted through Technology Center's fraud reporting portal located at: https://cccsecuritycenter.org/fraud-reporting.

Colleges have expressed hesitation in their submission of monthly reports due to concerns about disclosure. The Chancellor's Office, with guidance from state and federal authorities, has determined such communication may be kept confidential.

Colleges that do not report on monthly fraud activity will begin to see reminders sent to their Chief Information Systems Officers (CISOs) following the reporting deadline (i.e., the 10th of each month) with subsequent follow-up emails to the CEO. As such, CISO contact information should be up-to-date and reminders will be sent to the CISO list-serve membership. Appropriate college staff should use the information noted here for instructions on how to join or update their CISO list-serve contact(s).

Cooperation with Law Enforcement and Department of Education

The Chancellor's Office reminds colleges that they are required to report **all** fraud to the Department of Education, Office of the Inspector General (OIG). Fraud should be reported promptly to the OIG and colleges should engage with the SPAM filter, as such actions help protect all colleges. These data are invaluable to the OIG and others in both prosecuting criminals and updating the Office of Federal Student Aid's Suspect Information File (SIF), which informs the Institutional Student Information Report (ISIR) and is used as part of the student aid eligibility, verification and distribution processes.

The Chancellor's Office is encouraged by the Governor's recent 2022-23 budget proposal, which includes $25 million in ongoing and $75 million in one-time funds toward modernization of technology, including as it relates to the protection of sensitive data. All relevant information – from the Tech Center, through conferral with individual colleges and districts, workshops, participatory governance groups, and monthly reporting data – is being used to determine how best to support the system and allocate resources.

For additional questions or concerns related to the systemwide fraud mitigation strategy, please feel free to contact me at vlundywagner@cccco.edu or (916)322-1928. Colleges seeking additional more tactical support should contact the Tech Center Security Center staff at

securityhelp@ccctechcenter.org or by calling (916)431-0862, or reaching out to Stephen Heath, sheath@cccco.edu.

cc: Eloy Ortiz Oakley, Chancellor
Daisy Gonzales, Deputy Chancellor
Marty Alvarado, Executive Vice Chancellor
Lizette Navarette, Executive Vice Chancellor
Rebecca Ruan-O'Shaughnessy, Vice Chancellor
John Hetts, Visiting Executive