California Community Colleges

MEMORANDUM
June 22, 2021

DII 21-200-02 | Via Email

TO: Chief Executive Officers
Chief Information Systems Officer Association
Chief Student Services Officers

FROM: Dr. Valerie Lundy-Wagner, Interim Vice Chancellor, Digital Innovation and Infrastructure

RE: Admission Application Fraud and Financial Aid Fraud

The past year has presented numerous challenges for students, and also for colleges as they have supported the continuation of instruction throughout the pandemic. Unfortunately, the shift in course delivery format and remote work has contributed to an increase in efforts to undermine cyber integrity and an increase in fraudulent activity. The Chancellor's Office remains committed to the prevention of fraud, and this memo details the two types of fraud currently affecting the system, fraud prevention protocols currently in place, and the partnership required to strengthen fraud detection and mitigation.

Identifying Fraud & Fraud Types

The responsibility of preventing and identifying fraud is the work of every system stakeholder – the Chancellor's Office, the California Community Colleges Technology Center (Tech Center), districts, colleges, and relevant local departments. Preventing fraud without setting up additional barriers for real students requires a student-centered, guided pathways approach that engages the entire community.

CCCApply represents a critical part of the process to identify and mitigate fraud during the admissions and financial aid process. CCCApply currently uses a SPAM filter service to detect and identify the two related, but **different** types of fraudulent activity:

1. Admission application fraud, which occurs during the creation of a CCCApply account; and
2. Financial aid-related fraud, which occurs *after* a college has accepted an admission application and confirmed student identity.

This largely automated process is designed to observe suspicious patterns within admission application submissions and flags potentially fraudulent applications for review by college staff.

Every admissions application must first pass through the CCCApply SPAM filter service that is described in more detail on the Tech Center website.[1] To summarize, CCCApply identifies

[1] For documentation of the Spam Filter Web Service, please see the link here: https://cccnext.jira.com/wiki/spaces/PD/blog/2018/06/10/704315933/Development%2BSpam%2BFilter%2BWeb%2BService

potential SPAM (or fraud) and places it in a *Suspension* folder for each college with a notation of fraud_status = 3. Colleges are then expected make updates, that is specifically to review the *Suspension* folder and actively mark admission applications as "SPAM" or "NOT SPAM." The spam filter relies on machine learning to improve its effectiveness, making timely updates by colleges necessary to detect both types of fraud.

Financial aid-related fraud *only* occurs after a college has accepted an admission application. Therefore, it is important for the Tech Center to continue their work to improve CCCApply. It is imperative that colleges also revisit local protocols for reviewing and updating the SPAM filter, as well as confirming student identity prior to the release of financial aid. Reducing admission application fraud by reviewing the Suspension folder and making updates will quite definitively contribute to a reduction in financial aid-related fraud. Colleges are already required to report suspected Title IV fraud to the U.S. Department of Education's Office of Inspector General (OIG). Currently, there is no requirement for colleges and districts to report admission application fraud or financial aid-related fraud to the Chancellor's Office, or to actively engage with the CCCApply SPAM filter service.

Fraud Detection & Mitigation Strategies

Addressing both types of fraud will be an ongoing and long-term project for all system stakeholders. However, in the short-term colleges are encouraged to take proactive steps to protect themselves, their students, and the entire system. The Chancellor's Office will continue to work with the Tech Center to mature fraud monitoring processes and reporting, as described below.

Colleges

The Chancellor's Office strongly encourages colleges to review and update results of the CCCApply SPAM filter at least weekly. In particular, confirmed SPAM and false positive (valid application) SPAM results must be updated in a timely manner to improve the algorithm's ability to successfully characterize and detect fraudulent applications. This can be performed either through the CCCApply *Suspension* folder (i.e., changing the fraud_status value as relevant) or by sending a list of fraudulent application IDs to the TechCenter directly. Security incidents can be sent to the Tech Center by email to securityhelp@ccctechcenter.org or by calling (916)431-0862. In addition to reporting financial aid fraud to OIG, colleges should keep the Tech Center informed on the level of fraudulent activity occurring locally as it greatly improves our ability to provide needed support and respond appropriately. The Chancellor's Office will continue to be in close communication with the Tech Center to receive updates on fraudulent activity, use of the SPAM filter services and other issues.

Districts and colleges should eliminate inactive enrollment, per 5 CCR § 58004(c). **It is vital that faculty remove non-attending students by the Census date to significantly reduce the likelihood that financial aid is disbursed fraudulently.** Districts and colleges should also participate or present in relevant workshops on topics including updates on fraud detection, cybersecurity issues, and methods of fraud prevention.

Chancellor's Office & Tech Center

The Chancellor's Office and Tech Center are collaborating in at least three ways. First, the Fall 2021 release of CCCApply by the Tech Center will require two-factor authentication during account creation (for the admissions process). Common in other venues where identity verification is relevant (i.e., for personal banking), this additional level of complexity is designed to strengthen automated confirmation of real applicants. There is ongoing conversation about the extent to which this process will require phone numbers, as we recognize this may surface inequitable access to resources.

Second, protocols for identifying and reporting admission application fraud and financial aid-related fraud are being revisited. The Chancellor's Office is working to ensure that data needed to effectively monitor fraud are available, reported, and used to assess fraud mitigation efforts by the Tech Center and colleges. Issues of particular concern include the extent to which colleges are updating the CCCApply SPAM filter service and whether current reporting requirements are adequate to protect the system.

Third, the Tech Center and Chancellor's Office are in the process of acquiring and deploying advanced bot protection for web application firewall that should further secure account creation and submission systems. This firewall has history of use in combating unemployment fraud, so we anticipate positive results once this is deployed (anticipated sometime next month). Together, we will continue conducting research to identify technology solutions that could further secure account creation and submission systems. Such tools will be evaluated in the context of evolving enterprise architecture plans and readiness for implementation. The Chancellor's Office commits to keeping colleges abreast of any developments and encourages attentiveness to digital equity by the Tech Center, districts and colleges as fraud mitigation policies are developed and revised.[2]

For more support on fraud monitoring, detection, and prevention, colleges should reach out to the Tech Center, specifically: Dr. Jennifer Coleman, Director (jcoleman@ccctechcenter.org) or Jane Linder, Product Manager (jlinder@ccctechcenter.org). The Chancellor's Office also encourages colleges and districts to leverage state and federal emergency relief funds as they research, develop and implement sustainable strategies for monitoring and reporting fraud given the possibility of continued remote instruction and services going forward.

As we continue in this work to safeguard the system and provide needed opportunity available to aspiring and current students, please share this information with relevant colleagues, especially those in admissions and records, financial aid, and information security.

Should you have any questions or need further assistance, contact me at vlundywagner@cccco.edu or 916-322-1928.

[2] (Hancock, August 13, 2020). Digital Identification Must be Designed for Privacy and Equity. Electronic Frontier Foundation, retrieved from: https://www.eff.org/deeplinks/2020/08/digital-identification-must-be-designed-privacy-and-equity-10

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