Admission Application, Enrollment & Financial Aid Fraud

Prepared by:
Esau Tovar, Dean, Enrollment Services
Tracie Hunter, Associate Dean, Financial Aid & Scholarships
Teresita Rodriguez, Vice President, Enrollment Development

As you may have read in the Los Angeles Times on August 31 and this September 1 or heard about through listservs, several of our California Community Colleges have been inundated with fraudulent admission applications and enrollments. The driver appears to be associated with a financial aid scam, perhaps related to increased federal funding available to students during the pandemic.

First and foremost, I want to let you know that we are unaware of any active acts of course enrollment fraud or financial aid fraud at Santa Monica College. We believe the reason why Santa Monica College has not been the target of malicious financial aid activity is the result of strong anti-fraud preventive measures developed by the Enrollment Services and MIS departments at SMC within the past two years, as well as our enrollment payment policies. This is not to say we do not receive fraudulent admission applications—we do. Since adopting CCCApply in May 2017, we have identified over 60,000 fraudulent applications. These applications (and likely many other unidentified fraudulent applications) initially "passed" through screening/anti-spam measures instituted by the Chancellor's Office.

Details on admission applications and preventive measures we have instituted are provided below.

Applications and Fraud Status

As noted in Table 1 below, the number of domestic credit admission applications received by Admissions and Records has fluctuated significantly between 2014-15 and 2020-21 (based on WebISIS data).

In 2014-15 applications reached 98,201. From that year, until 2017-18 the number of applications declined from 1-3% each year. In 2018-19, we saw a 67% increase in applications, followed by another 54% increase in 2019-20, for an all-time high of 231,409 applications. However, applications declined once again in 2020-21 by 129% over the previous year to 101,273.

There are certainly many reasons that may explain this instability. Unfortunately, one of the most prominent reasons seems to be the number of fraudulent applications received since we migrated in May 2017 from our homegrown application to the California Community Colleges' CCCApply application for domestic credit students. Admissions and Records has received tens of thousands of fraudulent applications since then, which, unfortunately, still require processing and very often manual intervention.

Table 1. Admission Applications Processed

Year	Summer/ Fall	Winter/ Spring	Total	Percent Change Over Previous Year	Fraudulent Applications Identified	% Fraudulent
2014-15	67,282	30,919	98,201	-		
2015-16	67,133	29,668	96,801	-1%		
2016-17	64,286	28,425	92,711	-4%		
2017-18	60,528	29,389	89,917	-3%	1,428	2%
2018-19	94,522	55,734	150,256	67%	7,287	5%
2019-20	144,743	86,666	231,409	54%	35,073	15%
2020-21	70,359	30,914	101,273	-129%	18,601	18%

As noted in Table 1, the percentage of fraudulent applications we identified has ranged from 2% to 18% of the total received in a given academic year. However, thousands have likely gone undetected, especially among those submitted in 2019-2020 in what appears to be the height of our fraudulent admission application wave. It was in this year that MIS programmer, Fai Fong, and Admissions personnel (Esau Tovar, Michael Dammer, Mattie Lanz) devoted significant efforts trying to discern patterns of unusual or unexpected responses in application field/groups of fields that defied logic.

Some of the major patterns of fraud we recognized included the repeated use of sequential social security numbers, sequential email accounts, repeated phone numbers, and email accounts; non-existing mailing and permanent addresses; repeated use of IP addresses; IP addresses that are hosted in other countries; use of temporary email addresses, especially when the email provider has "spammer" reputation; use of state/country codes that do not correspond to addresses provided; among many others.

Recognizing these patterns is a time-consuming task as dozens to hundreds of applications must be reviewed and studied manually—field by field. Whenever patterns of suspected responses are identified, the programmer develops a query to look for that pattern in applications we have already received and flags them as potentially fraudulent.

All patterns identified to date become part of a fraud filter through which we process all our CCCApply admission applications. Those that get flagged are not automatically processed and the applicant is not sent an admission welcome letter. Instead, the applicant is contacted at the email address provided and is asked to provide proof of identity. Very few of these applicants indeed contact us. Those who do fall in one of two categories: legitimate student and "fraudster."

Legitimate students are assisted by Admissions personnel in correcting issues with their application, and their applications are processed as quickly as possible to enable them to proceed with the onboarding process. Fraudsters often call or email us to claim *their* SMC email address they say they purchased online, and they demand access to software that enrolled students have access to (e.g., Office 365 download). They tend to provide proof of identity passports or identifications that are fraudulent. Sometimes a simple google search reveals the very "identification" the applicant submitted.

It is important to note that SMC developed its anti-fraud algorithms because the Chancellor's Office was doing little in preventing the submission of fraudulent applications. It has been only in the last year that an anti-spam machine learning mechanism has been developed with the assistance of a technology firm. But this system relies on the work of individual colleges who must initially flag or confirm applications as fraudulent. SMC has submitted thousands of application identification numbers to aid in the task. Despite these efforts at the Chancellor's Office, thousands of fraudulent applications still get through and we must review them one by one to make a professional judgment of fraudulent/not fraudulent.

Of import to SMC, and a detriment is that the flagging of fraudulent applications is extremely time-consuming and our capacity to identify these is limited both in personnel available to review individual applications, as well as in our capability to discern response patterns of fraud at the individual application level and in the aggregate. While we can confirm many as fraudulent, it is simply not possible to do so on the majority given the available limited application data we receive, not to mention that instituting a universal identity confirmation requirement for all applicants would not be possible. Thus, the reason we only do so for applicants we strongly believe applied nefariously.

If we are to improve on the processes above, more personnel and the use of machine learning technologies are needed to further reduce the volume of fraudulent applications that get through.

Policies and Practices to Combat Fraudulent Enrollment

Notwithstanding the limitations above, we are confident that bad actors are not having complete "success" with their nefarious activities at SMC. In addition to our anti-fraud filters on the admission application processing program in WebISIS and the manual review of applications, we believe that two policies we implemented at the College have had great success at preventing major fraud (beyond application) such as that reported across other California Community Colleges; namely, course enrollment leading to financial aid fraud.

Limited Use of SMC Email Address

SMC has been the target of fraudsters and spammers seeking to exploit the added benefits that an SMC email account affords to students. Among these benefits is the ability to use and sometimes download Office 365, Adobe Creative Suite, and other software at no cost. The student email address also allows those who hold it to purchase software and other services through vendors that provide heavy student discounts, including Amazon, CollegeBuys, JourneyEd, OnTheHub, Academic Super Store, Apple Store, Best Buy, Dell, HP, Lenovo, Microsoft, Spotify, Huku, Adobe, GitHub, phone carriers, etc.

As a result of these tens of thousands of fraudulent applications, SMC changed its policy on how student email accounts are provisioned. Email accounts are now restricted from receiving messages from external domains (not "smc.edu"; with few exceptions). This largely prevents fraudsters from validating information that is typically a part of the account setup process with the vendor.

The SMC email address account is also initially precluded from sending messages to external addresses. This policy was implemented because bad actors were using student email accounts

with greater frequency for spamming purposes. Failing to act would have placed the College in legal jeopardy and loss of reputation for the smc.edu domain.

Once the student enrolls, pays their fees, and the term in which they enrolled is about to start, the student email account is given full privileges—both to send and to receive messages from external domains. These privileges are maintained so long as the student remains in active status.

After implementing the restrictions above in late October 2019 on new applicants' email accounts, we saw a major drop in applications received as evidenced in the volume of applications received in 2020-21. We knew that once bad actors learned about the restricted use of email accounts they would begin to lose interest in submitting fraudulent applications.

Payment Required to Keep Courses

The second policy that has minimized the impact of financial aid fraud is the requirement that students must pay for their enrollment fees by a specific payment deadline—before the start of the term (or must have been approved a fee waiver). Students who enroll after the initial payment deadline must pay their fees by midnight of the day they add a class, otherwise, they are dropped for nonpayment. Active enrollment is required to qualify for aid. Individuals who intend to commit financial aid fraud will likely not want to pay out of pocket to keep their classes.

It is important to note that the payment policy has some safeguards in place that help students who may not be able to pay their fees right away. Their expected financial aid award (based on Pell grant and loans, for example) is used as a temporary credit on their account, therefore preventing students with pending aid from being dropped. The College recovers these fees through the financial aid disbursement process.

Faculty Role in Fraud Detection

Faculty are important partners in the quest to keep bad actors from engaging in fraudulent behavior at SMC. Faculty are required to clear their rosters of "no shows" before the first census, which clears many of the "ghost" enrollees, however, as the numbers of fraudulent applications increased so did their sophistication. We have engaged faculty and have shared things to look for, especially now that so many classes are using remote modalities.

The following recommended best practices for managing enrollment in online classes, provided by the Chancellor's Office, were shared with faculty:

- Proactively reach out to students that have not engaged prior to dropping them from the course
- Hold and encourage early attendance in virtual office hours
- Review, at least briefly, any work submitted prior to Census to ensure it matches the subject matter being taught, or relates in other ways to the assignment the student was to complete.
- Be aware of oddities in enrollment, such as multiple students with the same phone number.
- Review student engagement and login frequency data in Canvas for online courses.
- Include real-time or near real-time interaction with students either during or outside of class

• For larger online classes, consider activities that are harder to automate responses to, including those that are separate from the course delivery platform, e.g., incorporating polling questions in Poll Everywhere or iClicker or using options within your local Learning Management System, such as a Canvas quiz.

Financial Aid

To date, the Office of Financial Aid & Scholarships has seen no evidence of Financial Aid Fraud. The department has safeguards in place to evaluate suspicious data. As it relates to federal grant aid, we have two disbursements per semester; where the second disbursement date is following the financial aid census date (usually the midpoint in the semester) after the faculty have confirmed their rosters. For the HERRF/CARES emergency funding, we do not begin awarding until after first census each semester to ensure that the students are enrolled in classes. When additional resources are available, we wait until late in the term to send a second disbursement, which rewards those who have persisted and futher eliminates the propensity for the bad actors.

In addition, the Department of Education has their own federal review process and selects students for an additional verification if any suspicious data is entered on the FAFSA. While we have seen an uptick in these additional verification cases, which has been the case nationwide and is believed that it is related to the fraudulent activities throughout the country, we maintain that currently our local, campus safeguards that are in place have addressed any suspicious activity.