THE STATE UNIVERSITY OF NEW YORK

APPLICATION, ENROLLMENT, FINANCIAL AID, AND SERVICE/DIGITAL RESOURCE FRAUD

SUNY Office of Risk Management and Compliance

SUNY Office of the Chief Information Security Officer

Issued 7-21-25

Updated 9-23-25 (see blue text in Appendix A)

Contents

Threat Briefing: Fraudulent Student Enrollments ("Ghost Students")

Overview:

Many higher education institutions are facing a surge of fraudulent student activities - admission applications, enrollments, financial aid applications and disbursements, and service/digital resource fraud (e.g., use of e-mail services, software licenses, etc.) carried out by cybercriminals using stolen or fake identities. These "ghost students" impersonate legitimate applicants to enroll in classes and claim financial aid or exploit campus resources. Their tactics have grown more sophisticated, often leveraging automation (bots) and large-scale identity theft to slip through admissions processes.

System Administration has received a number of reports of rising levels of fraudulent enrollments in the SUNY system and is in the process of collecting evidence and data concerning this issue.

This briefing outlines the tactics, real examples, and warning signs of such activity, and some initial recommended steps to spot and prevent fraudulent applications. We will continue this assessment and determine if any additional guidance or preventative measures are warranted and follow-up as more information becomes available.

Real-World Examples & Impact:

Fraud has impacted many higher education institutions nationally, in myriad ways:

- Organized Aid Theft:
    - The College of Southern Nevada (CSN) was hit by a ghost student ring in which fraudsters enrolled as "transfer students" and never attended class. Instructors reported full rosters but empty seats.
    - An audit found CSN had incurred $7.4 million in unpaid tuition and fees from these phantom students and had to repay the U.S. Department of Education for the federal aid that was stolen.

- California's Ghost Student Surge:
    - In the California Community College system, the scale of fake enrollments has been staggering. From July 2022 to June 2023, about 460,000 fraudulent applications were identified – roughly 20% of all applicants in that period.

- Los Angeles Pierce College saw its official enrollment plummet by 36% (7,658 down to 4,937 students) after purging known ghost students, indicating just how many fake students had been inflating its numbers.
    - "Ghost enrollment" not only threatened financial losses but also distorted planning: classes were added for illusory demand, at the expense of resources for real students.

- Other Reported Fraud Rings:
    - Maryland's Prince George's Community College reported a case where 80 fake applications were submitted in a single day – about one every 7 minutes.
    - Iowa Western Community College faculty grew suspicious of odd behaviors and uncovered 109 fraudulent enrollments in time to stop them.
    - These cases show organized scammers rapidly targeting institutions across the country. Many fraudsters are based overseas, treating U.S. colleges as targets for financial crime.

- Financial Aid Drained:
    - A recent comprehensive analysis by the U.S. DOE uncovered nearly $90 million disbursed to ineligible recipients, including thousands of deceased individuals receiving some form of payment indicating the direct fiscal impact of these schemes is significant.
    - During the COVID-19 pandemic, an influx of $40 billion in emergency student aid created a ripe opportunity – indeed, community colleges nationwide saw a wave of scammers post-2020 trying to capture relief grants and federal aid.

- Campus Resources Misused (Service/Digital Resource fraud):
    - For IT departments, ghost students translate into ghost accounts consuming resources.
    - At many colleges, each enrolled student gets access to email, servers, and software.
    - Large numbers of fake accounts can drive up licensing costs or cloud storage usage and increase security vulnerabilities.
    - Google and Microsoft have had to impose storage limits because fake student accounts are hoarding space.
    - Ghost students that linger on class rosters take up seats, potentially blocking legitimate students from registering for needed classes since seats are being falsely occupied. These tactics delay legitimate student's attempts to graduate in a timely manner.

- They distort institutional data (making it hard to know how many real students are interested or attending).

Combating Fraudulent Activities:

Raising Awareness through Education and Action:

While some SUNY campuses are already seeing patterns of fraudulent applications, registrations, and financial aid activity, others may not yet realize these schemes are affecting their campuses. Campus education will be key in combating fraudulent activities.

- **Inform front-line staff** (Admissions, Financial Aid, Registrar, IT, Faculty, etc.) about common fraud schemes.
- **Host a short briefing for** key offices on emerging patterns.
- **Distribute a campus-wide alert or guide** outlining indicators of suspicious activity – e.g., Appendix A - Tips for Identifying and Preventing Applicant, Enrollment, Student Financial Aid, and Service/Digital Resource Fraud).
- **Encourage faculty and advisors** to report non-engaged or unreachable students early in the term.
- **Ensure cross-campus/unit communication** — Develop a shared process for flagging and reviewing potential fraud cases.
- **Update training materials** for seasonal and student staff to include fraud awareness and escalation steps.

Technology:

- SUNY Community Colleges are encouraged to close their local applications and move fully onto the ApplySUNY app for the 2026 application cycle, at no cost to them or their students (see 7-9-25 e-mail to Community College Presidents, Chief Enrollment Officers, and Directors of Admission).
- This action will reduce the campuses' exposure to fraudulent application activity, and the need to mitigate. SUNY is developing additional measures around security currently, with a focus on defending ApplySUNY against the growing spate of attacks.

Notifications:

- **Notify the U.S. Department of Education**: See Steps to Take if Fraud is Detected here: Significant Actions to Prevent Fraud through Identity Verification | Knowledge Center.
- **Notify the SUNY Office of Risk Management and Compliance** of trends consistent with examples above (ORMAC@suny.edu).
- **Notify third-party vendors (e.g., admissions platforms, credentialing services transcript/diploma vendors, financial aid processors, etc.)** if you detect suspicious patterns.

Appendix A

Tips for Identifying and Preventing Applicant, Enrollment, Student Financial Aid, and Service/Digital Resource Fraud

Duplicate or Coordinated Applications:

- Fraud rings may submit multiple applications using slightly different names or demographic details.
    - Common indicators include the use of the same IP addresses or similar email patterns across many applications.
    - Sequential applications originating from out-of-state high schools.
    - Applications submitted for open majors with no prerequisite requirements.
    - Batches arriving in groups of 10–100, resulting in sequential ID #'s.
- Fraudsters often steal real identities and send transcripts from legitimate high schools to appear credible.
- Fraudsters hack high school and college systems to gain access to identities and then send real student transcripts to another institution to be used in a fraudulent application.
- Other suspicious signs include mismatched area codes, nonsensical or auto-generated email handles (e.g., jp.com. Justpr1.com, fanclub.pm).
- Bulk applications within specific age ranges such as 30–40 or 40–50 years old.
- Bulk applications from an address that is a one-bedroom apartment.
- Fraudsters using stadiums and movie theaters as home addresses on applications.
- An uptick in Social Security Numbers from particular states.
    - Prior to June 2011: The first three digits of an SSN, known as the "area number," did indicate the state where the applicant resided when they applied for the number. The SSA assigned area numbers based on geographic regions)Applications may also contain minimal information, such as no listed activities, a single unknown parent, identical self-reported GPAs, and no test scores.
- Many of these applications list local in-state addresses to qualify for fee waivers.
- Email addresses often follow a similar format, such as using the full student's name followed by numbers or characters (e.g., frittsjordan393@gmail.com or jordanfritts69y@gmail.com).
- Applications for primarily online education formats.

Identity Fraud:

- Fraudsters often use stolen identities, bots, and artificial intelligence to impersonate legitimate students.
- Indicators of identity fraud include mismatched personal information such as name, social security number (SSN), and date of birth (DOB).
- Repeated requests to change names, social security numbers, or DOB.
- Other red flags include the use of identities belonging to deceased individuals or incarcerated persons.
- Applicants may also submit AI-generated or altered documents, such as fake transcripts, diplomas, or passports.
    - In some cases, fraudsters request real documents on behalf of the actual document owners, such as having genuine high school transcripts sent to a college.
    - Additionally, some may present fake driver's licenses in person to support their fraudulent applications.

Academic Credential Fraud:

- Academic credential fraud involves the submission of fabricated or altered academic records.
    - This includes fake transcripts or certificates from unaccredited or non-existent institutions, manipulated grades or test scores, and fraudulent GEDs.
    - Applicants may also present degrees from diploma mills or unverified international institutions. For more information on identifying diploma mills, refer to resources such as AACRAO's Fraud busters initiative.
- Fraudsters may make online requests for credentials using generic or unusual email domains.
- They may submit repeated requests (especially transcripts) for different individuals to be sent to the same address (typically a third party).
- Fraudsters request that digital credentials be sent to free e-mail addresses not associated with real institutions (e.g., admissions@albany.gmail instead of admissions@albany.edu)
- Transcript requests accompanied by identity changes (e.g., name, DOB, SSN).
- The use of multiple credit card charges in short succession when attempting to send transcripts, diplomas, or other digital credentials.
- Failed payment attempts followed by attempts to use additional credit cards.

- Bulk or high-frequency transcript requests that do not align with normal student behavior:
    - Multiple requests from a single IP address or geolocation not tied to your student population.
    - Attempts to reroute transcripts after submission or ask for corrections without proper verification.
    - Schools should notify transcript, diploma, and credential vendors of suspected fraudulent activity.
- Duplicated or fraudulent requests for credentials (e.g., high school/college transcripts, diplomas, etc.)

Financial Aid and Residency Fraud:

- Fraudsters may misrepresent their dependency status, household income, or family structure to increase their eligibility for financial aid.
- They might also falsely claim state residency to qualify for in-state tuition rates.
- In some cases, multiple FAFSA applications are submitted using different identities in a coordinated effort to obtain aid.
- Fraudsters enroll in classes and remain active just long enough to receive financial aid disbursements.
- Fraudsters cash disbursement checks without attending classes or completing coursework.
- On the ISIRs, all applicants are marked as Independent, with two notable issues:
    - Data Retrieval Tool (DRT) was used, but the data is blanked out.
    - Data Retrieval Tool (DRT) was used, but no data was found.
- ISIRS come a day or two after the application.

SUNY The State University of New York