Monroe Community College
STATE UNIVERSITY OF NEW YORK

November through January, 2026 Issue 3

Institutional Compliance and Internal Audit Quarterly Newsletter

Compliance Matters

In this Issue

Inspiring every day.

Compliance in Focus

In this third issue of the Institutional Compliance and Internal Audit Office Compliance Matters, we will provide a brief update on MCC's compliance with the Annual Security & Fire Safety Reporting as required under the Clergy Act. Additionally, we will be taking a deeper dive into the phenomenon of fraudulent enrollment activities, referred to as "Ghost Student". We will explore what the term means, the impact it presents to higher education as a whole, and a review of SUNY's guidelines on how to combat this phenomenon. Finally, we will provide general updates on all policies and procedures adoption and revisions. Each quarter, the Institutional Compliance and Internal Audit Office will spotlight a specific policy or procedure to provide in depth review and update to the College community.

We encourage the campus community to actively engage with the Institutional Compliance and Internal Audit Office by providing feedback and suggesting topics you would like seen covered in future editions.

Thank you for being a part of this initiative as we work together to uphold the ethical standards that define our institution. We look forward to your participation and feedback!

Regards,

Institutional Compliance and Internal Audit

Spotlight: Clery Act and ASR

The Monroe Community College Annual Campus Security and Fire Safety Report (ASR) is available to all current and prospective students and employees on the Department of Public Safety website annually on October 1st. This report is part of the College's effort to meet the annual compliance requirements for both the Jeanne Clery Disclosure of Campus Security Policy and Crime Statistics Act and the Higher Education Opportunity Act, which require all colleges and universities that receive federal funding to provide the report on an annual basis. The report contains the statistics of campus crime for the preceding three calendar years and efforts made by the College to improve campus safety. Statistics must include information about incidents that occur on campus, public property within or adjacent to campus and in or on non-campus buildings or property that the College owns or controls.

SUNY's Effort in Combating an Increase in Ghost Students' Admissions

In recent years, higher education institutions have faced a growing challenge: the rise of "ghost students." This term refers to individuals who enroll in colleges and universities using stolen or fake identities, often to exploit financial aid benefits and campus resources without ever attending classes. According to an article on PBS, this phenomenon represents one of the most significant fraud challenges facing higher education institutions today. As fraudulent enrollment cost the nation millions annually, institutions including those within the SUNY system are developing comprehensive strategies to detect and prevent these fraud schemes. In this quarter's newsletter, we will explore what this phenomenon looks like, its implications for institutions, and how guidelines from SUNY and other institutions can help combat this issue at MCC.

What Are Ghost Students?

Ghost students are fraudulent enrollees who impersonate other individual's identity. Their tactics have become increasingly sophisticated, using automation and large-scale identity theft to navigate admissions processes. Linda McMahon, Secretary of the Department of Education, estimated that the country loses millions every year in fraudulent student aid for ghost students. On July 21, 2025, SUNY issued a 9-page document titled

"Application, Enrollment, Financial Aid, and Service/Digital Resource Fraud" (PDF), to help curb the increasing number of reports of fraudulent enrollments in the SUNY system. System have also issued various informational sessions through system-wide communication efforts like listservs, online training, and webinars in response to an uptick in fraudulent activities related to admissions and enrollments by bad actors.

According to guidelines, these fraudulent activities can include:

- Organized fraud rings who submit multiple applications using slightly different names or demographic details, often originating from the same IP addresses or email patterns with sometimes sequential student identification numbers, bulk applications arriving in groups of 10-100, and applications submitted from foreign locations are also common indicators.
- Fraudsters exploit financial aid systems to claim grants and loans they are not entitled to by enrolling in classes just long enough to receive financial aid disbursements, often never attending courses or completing coursework.
- Enrolled fraudsters may access campus resources like digital services, which can strain institutional budgets and services.

Real-World Examples & Impact

Fraud related to ghost students have impacted many higher education institutions nationally, in myriad ways, including:

- The College of Southern Nevada (CSN) was hit by a ghost student ring that racked up $7.4 million in unpaid tuition and fees, which led to the school repaying the Department of Education. This led CSN to implement a strategic enrollment verification process (PDF) to combat these types of incidents.
- In the California Community College system, between July 2022 to June 2023, over 460,000 fraudulent applications were identified, which constituted 20% of all applications during that period. Between March 2024 and March 2025, the California Community College Chancellor's Office tracked $10 million in federal and $3 million in state financial aid fraud.
- Los Angeles Pierce College saw its official enrollment plummet by 36% (7,658 down to 4,937 students) after purging known ghost students. During their spring 2025 semester, a criminal justice professor identified that 24 of 40 students in a single class were fraudulent accounts. Some ghost students used duplicated names, sequential student identification numbers, or profiles traceable to overseas networks. In one instance, the professor traced one student's profile photo back to a 24-year-old man who died in the 9/11 attacks.
- Prince George's Community College in Maryland, detected 80 fraudulent applications submitted in single day, which was about one in every 7 minutes.
- The U.S. Department of Education estimates nearly $90 million in federal aid has been disbursed to ineligible recipients "This isn't just about money," says Dr. Maria Chen, cybersecurity expert at the Center for Education Technology. "It's about trust in our educational institutions and their ability to protect both resources and real students' opportunities."

These fraudulent activities illustrate not only the financial repercussions of ghost students but also how they can distort enrollment data and resource allocation and increase security vulnerabilities. Both Google and Microsoft have imposed storage limits because fake student accounts are hoarding space, per a report published in Ed Tech Magazine. 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 students' attempts to graduate in a timely manner. They distort institutional data (making it harder to identify how many real students are interested or attending).

Combating Fraudulent Activities: Raising Awareness through Education and Action.

SUNY noted that some of its campuses are experiencing "*patterns of fraudulent applications,* *registrations, and financial aid activity",* but pointed out that "*others may not yet realize these schemes are affecting their campuses*". To help combat these fraudulent enrollments activities, SUNY's Office of Risk Management and Compliance has established detailed guidance for detecting and preventing fraudulent activities across the system. SUNY's approach centers on three primary strategies: institutional awareness, technological solutions, and coordinated response protocols. SUNY emphasizes the importance of educating front-line staff in admissions, financial aid, and registrar offices, IT departments, and faculty about common fraud patterns. They recommend hosting briefings for key offices on emerging patterns and distributing campus-wide alerts outlining indicators of suspicious activity. Faculty and advisors are encouraged to report non-engaged or unreachable students early in the term, and cross-campus communication processes should be developed for flagging and reviewing potential fraud cases. SUNY guidance specifies numerous indicators of potential fraud:

- Duplicate or coordinated applications with sequential ID numbers or identical demographic patterns;
- Applications originating from non-sequitur addresses (stadiums, movie theaters, one-bedroom apartments);
- Mismatched personal information (name, social security number, date of birth);
- Requests to change identifying information repeatedly;
- Use of AI-generated or altered documents, including fake transcripts or passports;
- Financial aid applications where all applicants are marked as Independent with blanked-out or missing Data Retrieval Tool information; and
- Bulk applications for primarily online education formats

Beyond classroom seats, ghost student accounts drain institutional resources. Each enrolled student typically gains access to email account, cloud storage, and software licenses. SUNY noted these fake accounts increase "*licensing costs, cloud storage usage, and create security vulnerabilities"*

Recommended Preventative Measures

SUNY's framework includes specific notification and escalation protocols. When fraud is detected, institutions must notify the U.S. Department of Education, the SUNY Office of Risk Management and Compliance (ORMAC@suny.edu), and relevant third-party vendors such as "*admissions platforms, financial aid processors, and transcript vendors*". This coordinated approach enables the identification of patterns across the system and allows vendors to strengthen their security measures. The guidance also emphasizes the importance of enhanced identity verification. Federal requirements announced in June 2025 now mandate that an applicant for federal student aid present valid government-issued identification either in person or via live video verification. SUNY institutions are encouraged to implement digital verification platforms and maintain alternative processes for applicants under 18.

At MCC, the College is reviewing its verification processes to help curb these types of fraudulent activities from occurring at our campus.

Policies, Procedures, and Protocols

The Institutional Compliance and Internal Audit Office strives to bring awareness to MCC Community about new and updated college-wide policies, procedures, and protocols. The College's Policies, Procedures, and Protocols website is designed to answer many questions you may have concerning MCC's stance, which is aimed at advancing its mission and goals.

MCC's policies, procedures, and protocols undergo a thorough shared governance review process once every five years (with some exceptions). Each College division is represented by an individual within that division. Any questions are concerns can be directed to the Policy Division Representative. Additionally, the Institutional Compliance and Internal Audit Office is responsible for the administration of the policies. Should you have any questions, you can direct them to: Compliance and Internal Audit Office (complianceandaudit@monroecc.edu).

Recent new and updated policies, procedures, and protocols include:

New Policy/Protocol:

- Anti-Hazing Policy (PDF)
- Student Club and Organization Social Media Protocol (PDF)

Revised Policy/Protocols:

- Social Media Protocol (PDF)

Take a moment and visit, MCC Policies webpage for more information.

About *Compliance Matters*

Compliance Matters is a publication from the Institutional Compliance and Internal Audit Office. This issue marks the 3rd volume of the publication. The Institutional Compliance and Internal Audit Office provide relevant compliance content across the campus Community. Any feedback or suggestions for improvement may be directed to the office's general email address: Compliance and Internal Audit Office (complianceandaudit@monroecc.edu).

Meet the Team

- Brenda Ronan, Institutional Compliance Officer & Internal Auditor
- Karen Chin, Project Director