

# Fraudulent Applications & Sensitive Information

## February 5, 2025

### Fraudulent Applications

A perfect storm of circumstances has led to a significant increase in fraudulent applications, in higher education, from so called “ghost students” or “Pell runners”. Community colleges have been particularly vulnerable – scammers apply for federal and state financial aid, pocket the funds and vanish without ever attending classes.

With the pandemic of 2020, institutions saw the prevalence of online scams. There was a shift from in-person to online and hybrid learning as well as the rise of AI (artificial intelligence) technology. This shift also made it difficult for professors to confirm the actual attendance rates of their students.

### How it Works

Ghost students are not real students. They are created by scammers often using stolen identities, social security numbers (SSN) and fabricated academic records to generate fictitious student profiles and apply for enrollment. Scammers employ bots or automated systems to submit multiple applications quickly, often targeting community colleges and online programs where admissions barriers are lower.

Upon acceptance, “students” apply for aid through FASFA (Free Application for Federal Student Aid) and stay in class until the census date, doing the bare minimum to remain registered, even using AI to generate essays, and avoid being dropped from a class for non-participation. Once the financial aid is disbursed, the “student” withdraws the funds and vanishes. Pell Grants, which do not require repayment, are a common target because they are ideal for immediate financial gain.

With acceptance, they also gain access to other institution provided resources, such as: cloud storage or VPN and student (.edu) email addresses to help them carry out other potential scams.

### Operational Impact

According to [Cybersecurity Ventures](#), global cybercrime costs are projected to skyrocket from \$9.5 trillion USD in 2024 to \$10.5 trillion by 2025. In 2024, several high-profile data breaches (e.g. AT&T, U.S. government agencies and universities and Bank of America) compromised organizations across various sectors. These breaches contributed to billions of people’s data being published on the dark web for ghost students to use.

Since 2010, community colleges and higher education institutions have flagged an estimated 20% to 36% of their student populations as potentially fraudulent. This practice has cost educational institutions millions and has prevented legitimate students from accessing online courses. In California, the problem has become so prevalent the U.S. Department of Education has been looking into the matter, with 48 investigations currently in progress.

## Key Indicators of Fraudulent Financial Aid Applications:

- Unusual patterns in address or email usage
- Sudden surges in applications
- Inconsistent borrowing amounts
- High withdrawal rates among students with Parent PLUS Loans (PSL)
- Suspicious FAFSA submissions
- Multiple student refunds going to the same account
- Discrepancies between reported income and loan amounts
- Clean ISIR (Institutional Student Information Record) records despite fraudulent documents
- Varying levels of student engagement based on fraudulent rings
- Registration for classes without prerequisites
- Forged Document Submission
- Identification of copied or pasted content within the application
- Identification of multiple applications originating from the same IP (Internet Protocol) address

The ongoing fight against fraud requires continuous modernization and vigilance, ensuring opportunities meant to help students are not exploited by bad actors. The complexities of shifting between in-person, virtual and hybrid learning have been met with an increasingly complicated and evolving cyber threat landscape where colleges have become primary targets of cyber threat actors.

Combating fraud is best accomplished through meaningful cybersecurity investment. The stakes are too high to ignore, and the tools to address these challenges are readily available. By prioritizing software such as: multi-factor authentication (MFA), biometrics and other types of identity security tools, institutions can ensure they remain a place of integrity and excellence in education.

## Reminder: Emailing Sensitive Information & Documents

We have noticed an increase in emails, with attachments requesting sensitive information, being blocked in Barracuda, McLennan Community College's (MCC) SPAM filter.

Barracuda is set up to filter incoming/outgoing emails to help protect MCC from potential harmful content, files, and data leakage. Sensitive information such as: social security numbers (SSN), W-2s, dates of birth (DOB), credit card numbers, bank account information, etc. will trigger a block if detected.

---

Revision #2

Created 17 March 2025 18:51:10 by Laura J. Crapps

Updated 2 April 2025 13:28:17 by Laura J. Crapps