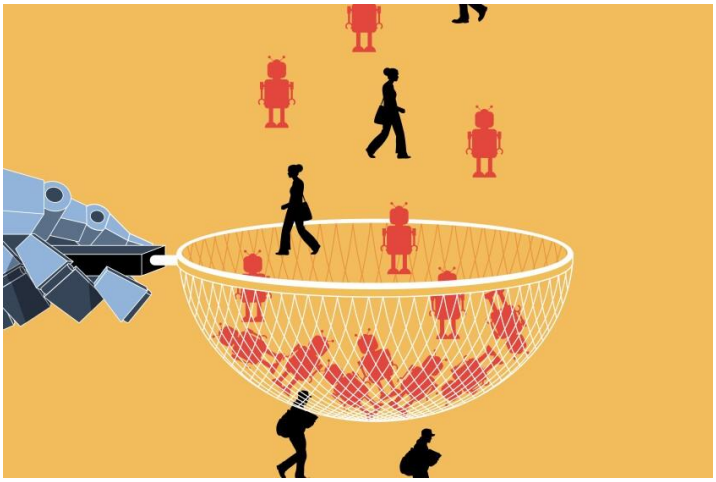
THE CHRONICLE
OF HIGHER EDUCATION

Admissions Fraud (Article link)

Colleges See Alarming Rates of Fake Applications. So They're Turning to AI.

By Taylor Swaak October 1, 2024



Fraudulent admissions applications are routine for Ron Weist.

On a particularly busy day recently, Weist said, fraudsters sent 80 fake applications to Prince George's Community College, in Maryland — one every seven minutes for a couple of hours. But that number seems less daunting than it might have just a few years ago. That's because Weist, the college's customer-relationship management (CRM) administrator, is now catching most of those bad actors on the front end, screening them out with technology supported by artificial intelligence.

So are a few hundred other U.S. colleges.

"It's really kind of letting technology do what it does best, so our people can do what they do best," Weist said. So-called "ghost students" have plagued many colleges in recent years — a phenomenon driven by motives such as financial-aid fraud and access to student discounts for services like Adobe Creative Cloud and the Microsoft 365 suite. The Covid pandemic, in particular, introduced additional risk factors for fraud: pivots to purely online learning and $30 billion from the Higher Education Emergency Relief Fund, or Heerf, for colleges to disperse to students.

Community colleges have been especially vulnerable to these attacks. Their mission to make education accessible to all students — through practices like open admissions, no application fees, and low-cost tuition that maximizes the amount of Pell grant and loan refunds a student can receive — makes them an attractive target, said Mark Kantrowitz, a nationally recognized expert on student financial aid. Some of the better-known victims are California's community colleges, which have collectively lost millions to such scammers since 2021.

The resulting harm goes well beyond lost financial aid, though. Fraud is "wasting the time and staff at these community colleges," Kantrowitz said. "So they have a fairly strong incentive to crack down on this."

The solution, for some, has been AI software that can be integrated into a college's application-processing system — acting somewhat like a sieve. These tools can, among other things, cross-reference an applicant's information with public records and commercial data. And when fraud is identified, the tools retain that information, effectively "learning" fraudsters' patterns and behaviors to improve their detection capabilities.

But these tools aren't infallible. College administrators said human checks are still critical to ensure these technologies don't inadvertently block real students who want to enroll.

“If a student gets an email that their application has been flagged, and to call us — that might be enough of a barrier where they don’t go to college,” said Scott Fiedler, college registrar at Ozarks Technical Community College, in Missouri. “It’s really high stakes.”

A Threat Emerges

The application process at many community colleges with open admissions is like this: A person fills out an application, clicks “submit,” and within seconds that application is automatically accepted. The applicant is moved to a student-information system (SIS), where they’re given an email address and a student ID. Admissions and enrollment folks then review documentation such as transcripts and test scores, and request additional verification if something seems amiss.

This process, while imperfect, has worked — until, for some, it didn’t.

For Weist, at Prince George’s Community College, the wake-up call came just before the spring of 2021. It was 20 days before the start of classes, and the number of applications was up 27 percent from that time the prior year. He and his colleagues celebrated, Weist recalled. Popped the metaphorical champagne bottles. Congratulated themselves on a recruiting job well done amid a grueling pandemic.

Then, about a week later, Weist hit refresh and saw the percentage had spiked to 47 percent. “I had one of those moments where my heart just sank,” Weist said.

At Louisiana Delta Community College, Nathan Hall, the dean of enrollment services, also noticed a higher volume of applications around that same time. His team started conducting fraud-specific “purges” of students in the system twice a year, homing in on those who, for example, had applied with non-local addresses and were enrolled only in classes without degree restrictions. Those purges would each wipe out between 200 and 350 students (the college serves around 4,000 learners).

These breaches were more than just a nuisance. They posed a cybersecurity threat and compromised data integrity. And, most notably, they drained colleges’ time and resources.

At Prince George’s, fake students were displacing actual students trying to take classes, Weist said. The college even hired additional adjuncts on a few occasions to teach courses where — unbeknownst to anyone at the time — the majority of students were actually fake.

Rebecca Wojcicki, manager of admission operations at Oakton College, in Illinois, said two people on her small team started manually reviewing every application submitted between August 2023 and June 2024 — a process that doubled the time they normally spent processing applications. By the end, they determined that about 21 percent of the applications were fraudulent.

None of the sources *The Chronicle* spoke with for this story said they had evidence that these fake students had successfully stolen any institutional or federal aid.

Federal student-aid fraud *is* something the government tracks (and that institutions are required to report). While the Education Department’s Office of Inspector General wouldn’t provide counts of reported fraud by year without a public-records request, Catherine Grant, a public-affairs liaison, confirmed in an email that “the number of student-aid fraud allegations received by our office has increased” over the last decade. (She noted that several factors, including heightened awareness of student-aid fraud, could explain the change.)

The office has publicized at least 10 cases of fraud linked to fake applicants on its site since 2022, with estimated damages for each ranging from $36,000 to more than $5.6 million.

Turning to AI

With clear stakes for colleges, admissions and enrollment administrators started looking for technological help — just as the market for AI products was heating up.

At the time of publication, AI software on *The Chronicle*'s radar with active U.S. college clients are AMSimpkins & Associates' S.A.F.E., BM Technologies' (BMTX) Identity Verification, and Ellucian's Apply. The S.A.F.E. software rolled out in late 2022; the other two products became available earlier this year. (For now, Ellucian's Apply is optimized for users of the company's existing suite of tech solutions.)

While each software has unique strengths and its own "special sauce," as one company vice president for sales put it, the way they work is fairly similar. These software integrate with a platform a college is already using, such as a CRM system like Salesforce or Slate, and screen applications as they're submitted.

During this process, parts of an application — first name, last name, address, phone number, email address, date of birth, etc. — are cross-referenced against a host of public and/or commercial databases, including voter-registration databases, telephone directories, realtor sites, utility and email service providers, and global watchlists.

Do the name and address not line up? That's a flag. Is the phone number on a spam list? That's a flag. Is the address provided actually for a commercial property, a vacant lot, or a property for sale? That's a flag. (Spokespeople for the companies noted that applicants' information is encrypted to safeguard personal information.)

These software ultimately place applications into categories — like pass, review, or fail — based on the various parameters established within the tool. The latter two statuses will stall an application's progress. Clients are then able to review and verify those recommendations, and can also manually change the status if they deem that appropriate.

Company spokespeople underscored that where these technologies really shine is in their ability to retain information, and learn. So if, say, an IP address a fraudster uses is flagged at one college, that address will be flagged if the fraudster attempts to apply again, or attempts to apply to other colleges that use the same software.

College administrators *The Chronicle* spoke with said it's unclear — or too soon to know — if having these software deter fraudsters. (Most don't publicize their use of this technology to applicants.) What *is* clear, though, is that the tools are catching bad actors who might otherwise covertly enroll.

At Louisiana Delta, for example, which began using BMTX's Identity Verification on August 30, the tool has helped prevent about 500 fake applications from getting through, Hall reported. He added that this was outside of the season when they'd get the most applications, too.

At Prince George's, which has been using S.A.F.E. since March 2023, the software has blocked some 6,300 fake applications — about one in eight applications that the college receives.

Not a Panacea

Even so, administrators said human beings remain a critical part of the process. That's because these software can, and sometimes do, flag real applications.

At least part of this, it seems, has to do with the fact that community colleges serve many nontraditional students, which can complicate data verification. At Louisiana Delta, for example, Hall noted that some applicants who live in temporary housing or with a friend get dinged because their name and address don't align. Colleges also have to be mindful about whitelisting IP addresses for public places like schools and libraries, where prospective students may be using shared devices to apply.

Ozarks Technical Community College, which uses the S.A.F.E. software, has had issues with high error rates, or instances where an application flagged as needing review or failing is later cleared after a manual review. This includes applications from minors. The college serves more than 1,000 students under age 18 through its dual-credit programs, and when minors apply, the software flags them as not being verifiable through public records.

Jonathan Grindstaff, a programmer analyst at Ozarks, reported that since adopting the tool in January, the team has moved about 58 percent of applications marked "fail" and 77 percent of applications marked "review" to the pass pile.

"It's a starting point for us," but "I don't know that it'll ever get to the point where it's 100 percent accurate," Fiedler, the college's registrar, said. "There are too many variables."

(Tyler Merwin, senior account executive at AMSimpkins & Associates, wrote in an email that S.A.F.E. clients "set their own specific settings and weights" that can influence which category an application falls into and the resulting error rate. He added that clients can adjust at what age an applicant gets flagged.)

Wojcicki, at Oakton, which uses the S.A.F.E. software, said while the tool is meeting her team's needs, she's also eyeing additional capabilities, such as verification of corresponding documents like transcripts, test scores, and driver's licenses. Submission of fake documentation is "still under the fraud umbrella," she said, and "it's an issue that many schools are also facing and have had discussions about." (None of the three software providers mentioned provide this service, but all noted that it is part of their development plan. S.A.F.E., in particular, stated it plans to roll out such capabilities by next year.)

Beyond third-party AI tools, Weist hopes that a more "national solution" and response emerge to combat admissions fraud. Guidance and standards to start — maybe even a federal-level task-force. Because even though his college has found a tech solution that tackles the problem head on, it doesn't eliminate the problem.

"We've done a good job, but make no mistake," he said. "It's a lift."

View Article Online

About the Author

Taylor Swaak is a senior reporter at *The Chronicle of Higher Education*, covering how institutions are harnessing technology to innovate. Learn more.

DMI – 10/28/2024