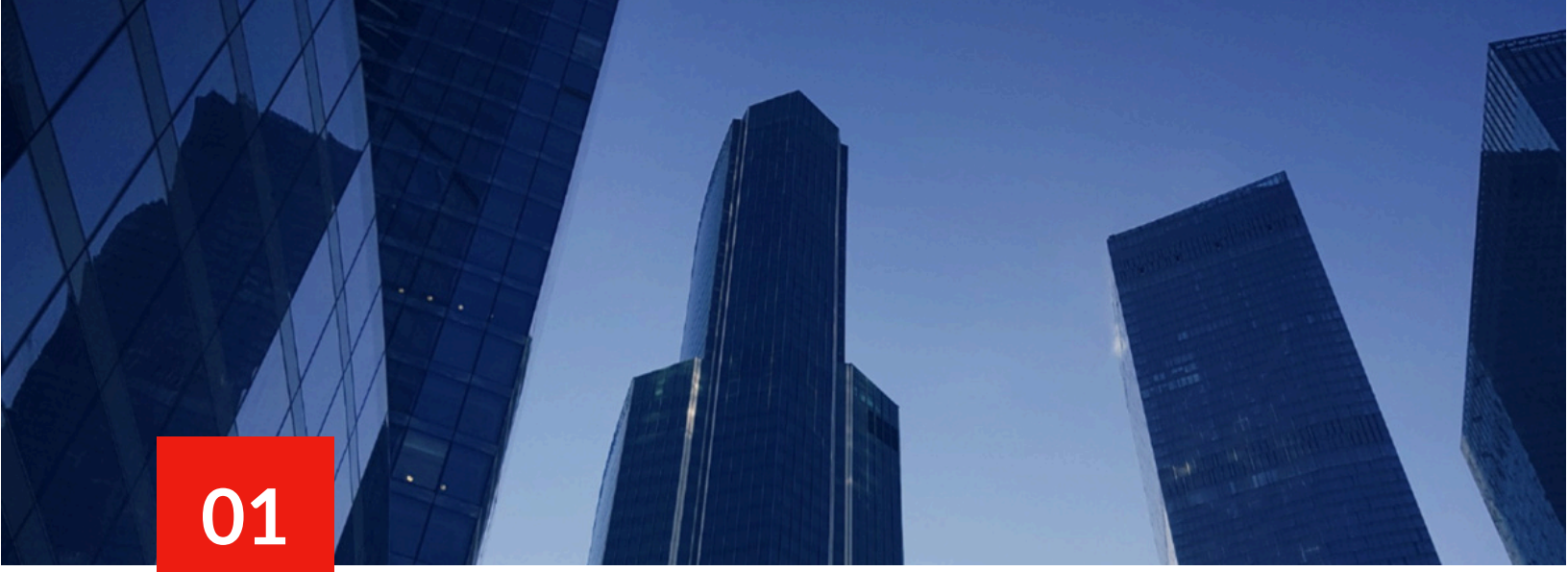


01

Introduction

Scammers posing as fake students are inundating colleges across the U.S. with fraudulent applications. Using stolen or fabricated identities, these "ghost students" successfully enroll, only to disappear—tying up course seats, stealing financial aid funds, and securing official college-issued email addresses.

While the recent surge in ghost students is often attributed to widespread adoption of online classes, there are many contributing factors:

- Efforts to streamline the application process, like user-friendly online applications with no application fees and automatic enrollment, can also open doors for fraudsters.
- Widespread data breaches, including the exposure of tens of millions of K-12 students' data via the PowerSchool hack, supply fraudsters with plenty of data to craft convincing identities.
- AI tools make it easier for scammers to automate the application process, generate fake documents, and even submit basic coursework to evade detection.

The Department of Education reports that about $90 million in aid was doled out to ineligible students over the past three years. California has been particularly hard hit— $13 million in financial aid was reportedly stolen by fake students over the last year alone.

Fraud on this scale erodes public trust, damages the reputation of educational institutions, and deprives legitimate students of the resources they need to succeed.

Though there is growing awareness of the problem, many colleges still lack the real-time analytics, document verification infrastructure, and fraud detection strategies needed to proactively identify threats and comply with evolving regulations.

This report will examine the long-term effects of application fraud, explore the increasingly sophisticated nature of fraudsters' tactics, and share actionable strategies for keeping ghost students out of higher education.

$90M

in fraudulent payments

The Department of Education reports that about $90 million in financial aid was doled out to ineligible students over the past three years.

02

An administrative nightmare for more than admissions

Application fraud creates a massive administrative burden that saps resources and distracts staff from their core mission. Instead of helping students navigate the complexities of applying, enrolling, and securing funding for tuition, admissions and financial aid staff are increasingly spending their time verifying student identities and manually searching for signs of fraud.

Despite advancements in technology and automation designed to streamline admissions, more than 90% of staff are devoting more time to application processing than they have in the past five years, according to a study conducted by the Association of Student Financial Aid Administrators (NASFAA).

> 91% of respondents to NASFAA's 2025 Administrative Burden survey reported feeling the time and resources their office devotes to processing each aid application has "greatly increased" or "somewhat increased" in the past five years.

Instructors' administrative workloads are also affected by ghost students, especially those who teach online or hybrid courses. Many instructors report wasting time interacting with bots. Wendy Brill-Wynkoop, a professor at College of the Canyons in Santa Clarita, explained that "Bots are getting so smart, they're being programmed in a way that they can even complete some of the initial assignments in online classes so that they're not dropped by [the deadline to drop the class]."

To avoid these downstream administrative nightmares, schools must invest in intelligent solutions that stop ghost students at their point of entry—the application process. We'll dive deeper into strategies to do just that later in the paper.

03

Fake student data affects budgeting, student services, and overall planning

As institutions struggle with enrollment and funding, campus leaders are turning to data to make more informed strategic decisions that will improve student success and enhance operational efficiency. Educause's 2024 Higher Education Trend Watch found that calls for more data-informed decision-making were a primary concern for higher education IT leaders. Faculty and staff across departments are also seeking accurate data, and many IT organizations are focused on making data more usable for all stakeholders.

Fostering a culture of data-informed decision making is crucial for organizational health, but application fraud dooms this effort from the start. An inaccurate headcount alone will lead to incorrect enrollment projections, which will negatively impact financial planning and resource allocation.

There are downstream impacts as well. For example, higher education leaders might analyze data related to course popularity, drop rates, and completion to ensure that their course offerings align with student demand. Their conclusions, though, will be useless if ghost students account for even a portion of enrollees.

Fake applications can also affect funding, particularly for schools in states where funding is based on a combination of enrollment and performance metrics like course completion and graduation rates. Ghost students can artificially inflate enrollment numbers while simultaneously depressing completion rates, skewing this data and the funding calculations.

Can you spot the imposter?

An art history instructor who teaches for one of Voyatek's clients noticed that her online upper level art history class which was mainly taken by art majors was full and had a waiting list. In her 20 years of teaching, she never had more than 6 to 8 students.

As wonderful as it seemed, she thought something was wrong and alerted the school's registrar and IT teams. Her art history class was full of ghost students, who enrolled and picked up her fully online class since it appeared first on the alphabetical list of online courses.

04 Application fraud damages schools' reputations and hinders efforts to build public trust

The declining trust in postsecondary education is well-documented. Though Gallup's annual study showed a slight increase in Americans' confidence in higher education this year, less than half (42%) of respondents said they have "a great deal" of confidence in it. Nearly a quarter (23%) said they have little or no confidence in higher education.

Institutions that fail to expel ghost students are putting their reputation at risk. Application fraud is particularly detrimental to public trust because it damages an institution's reputation at both the micro and macro levels.

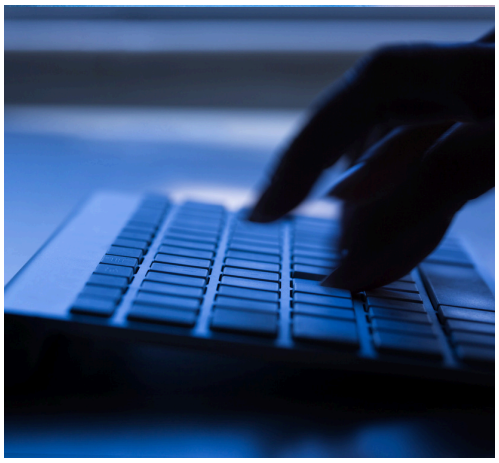
At the micro level, application fraud directly affects newly enrolled and current students. Ghost students monopolize required courses and prevent faculty from supporting real students. They steal financial aid from the federal government, state governments, and the institution itself. Once enrolled, fraudsters can also access internal systems, stealing students' personal and financial data.

At the macro level, the public expects higher education to protect student data, be responsible stewards of taxpayer dollars, and deliver programs that help students succeed. Application fraud hinders the industry's ability to meet these expectations. For Americans who are already skeptical of the cost of higher education and critical of colleges' ability to prepare students for the workforce, headlines about college systems losing millions in fraud have an outsized impact.

Columbia University Hacked

A recent hack of Columbia University's computer system compromised the personal information of hundreds of thousands of people, including students and applicants.

More than 870,000 individuals were affected by the breach.



05

Ghost students aren't going away

These long-term problems are the result of a long-term effort. Application fraud is perpetrated by organized criminal networks operating at scale, sharing information and learning from each other's successes and failures. Socure, the identity verification firm that Voyatek partners with to help our clients combat application fraud, conducted an in-depth study of ghost student activity and found that these attacks are much more sophisticated than an average identity fraud scheme. Fraudsters use automation bots, VPNS, and proxy servers to mask their origins. They predominantly leverage real victims' personal data, rather than fully fabricated identities, which further helps them fly under the radar.

In other words, the ghost student problem is an identity verification problem. To address it, institutions need to find out who is really behind the computer.

Unfortunately, existing identity verification solutions can miss red flags and create frustrating roadblocks for legitimate students. For example, many identity verification providers rely exclusively on optical character recognition (OCR) to extract text and validate a document's authenticity. But OCR can lead to errors, like mistaking a "Cl" as a "D" on a blurry passport photo. In this case, Clara becomes Dara, and Dara's verifying documents don't pass muster. Now, Clara and the application staff tasked with manually re-checking her documents are frustrated.

To stop ghost students without penalizing real students, colleges need to invest in advanced identity verification.

Relying exclusively on optical character recognition (OCR) to extract text and validate a document's authenticity without examining the veracity of the data itself leads to many false positives.

06 The solution: Advanced, AI-Enabled Identity Verification

A scalable strategy for protecting higher education systems begins with embedding identity verification and fraud prevention directly into admissions and financial aid workflows. The goal is to passively confirm that applicants are legitimate students while minimizing friction for genuine users. When risks are detected, applicants can be escalated to additional verification steps—such as submitting a government ID, a live selfie check, or device and location analysis—to ensure consistency between claimed and actual identities.

This kind of layered approach—combining passive checks with progressive, step-up verification only when needed—balances accessibility with security. It reduces the burden on institutions, prevents fraudulent applications from slipping through, and helps ensure resources are directed toward real students.

Solutions like Voyatek's Application Fraud Firewall use hybrid verification methods—including predictive fraud modeling, document validation, and device fingerprinting— to analyze admissions, financial aid, and enrollment data and identify fraud with precision and accuracy, dramatically reducing processing times and manual reviews.

> Usually, when you buy a new solution, everyone is afraid of the level of effort involved.
>
> But the implementation process for Application Fraud Firewall was a great experience. The Voyatek team was great to work with, understands financial aid data, and there was minimal impact on IT.
>
> *~Tom Bilbruck, Associate Dean, Student Financial Services, College of the Canyons*

07 Application Fraud Firewall

To tackle increasingly complex fraud schemes, Application Fraud Firewall:

Leverages unified data models to expose identity anomalies across systems, not just admissions.

Many existing solutions begin and end fraud detection within an institution's admissions system, limiting results. Application Fraud Firewall consolidates application data from on-premise and cloud-based systems, including CRM, SIS, and LMS, then ingests and correlates identity signals—such as PII reuse, contact detail frequency, device/IP patterns, and behavioral outliers.

Detects coordinated identity fraud by tapping into shared signals and graph-driven insights of risks accross a variety of industries.

Using Socure's best-in-class predictive models and proprietary set of data sources, Voyatek's platform analyzes every facet of a digital identity, utilizing over 1000 data sources, 17,000 features, 8 billion rows of data to continuously track fraud signals. These signals —spanning identity, device, behavioral, and transaction metadata—are continuously enhanced through operational feedback loops, improving precision at both the institutional and industry levels.

Meets current demands and adapts to future compliance needs.

With federal identity verification mandates still in flux, institutions must prepare for a range of possible futures (e.g., the requirement of Identity Assurance Level (IAL) 2 digital flows) while stopping the fraud that is at the door now.

Built for Higher Education

Voyatek's Application Fraud Firewall's models continuously learn from thousands of data sources, spanning finance, healthcare, gaming, insurance, payroll, telecom, and others that accurately represent the online life of the typical college applicant.

Our team tailors our solution for each institution's specific environment, working closely with internal IT teams to comply with data integrity and security policies. This results in an architecturally adaptable system, defensible decisioning, and assurance that your institution can scale quickly and securely in response to regulatory changes—without operational disruption.

This approach further strengthens and protects workflows outside of admissions in which accurate identity verification is critical, like processing transcript requests and hiring remote employees.

ONBOARDING ...AND BEYOND

ADMISSIONS APPLICATION

FINANCIAL AID APPLICATION

PASSWORD RESET/ ACCOUNT RECOVERY
Email / phone risk

REMOTE PRESENCE TRANSACTIONS
New bank, transcripts, online exams, etc.

A 2025 Gartner report predicted that by 2028, one in four candidate profiles worldwide will be fake, largely due to AI manipulation.

1.1 million students

Voyatek has served 80 higher ed institutions, supporting more than 1.1 million students nationwide.

Our clients rely on our AI-powered solutions to prevent fraud, advance enrollment initiatives, optimize staff performance, and improve institutional health.

Voyatek

Get a Fraud Health Check

Want to learn more about Application Fraud Firewall? Try out our Fraud Health Check service. We'll run our models on your data and share the results in a private demo environment.

Contact us today to learn more from one of our higher ed experts.

Learn more about the Fraud Health Check.

John Van Weeran
Vice President, Higher Education
(571) 723-4205
john.vanweeren@voyatek.com

Kelley Bradder
Chief Information Officer
(515) 419-1072
kelley.bradder@voyatek.com

Emily Bonham
Senior Analytics Manager, Higher Education
(443) 380-3626
emily.bonham@voyatek.com

Casimiro (Casey) Lovato-Winston
Technical Expert
(916) 612-8840
casimiro.lovato-winston@voyatek.com