Admissions Denied: How to Prevent Admissions and Financial Aid Fraud in Higher Education

CONDUCIVE | splunk> a CISCO company | carahsoft

Introduction

Ghost students. Pell runners. Synthetic identifications. All these terms have one thing in common: They involve waves of students who vanish after financial aid disbursement.

Each year, colleges and universities receive thousands of applications, but only recently have administrators had to ask if they're all legitimate. Fraud in higher education is on the rise, and automation and **AI have made it easier than ever for bad actors to quickly submit applications**, giving rise to fake students.

On paper, they look like real students — with a seemingly real name, address, phone number, social security number, transcripts, test scores, and a completed Free Application for Federal Student Aid (FAFSA) form. Yet, once schools accept them and release financial aid, they disappear, draining the resources of your already strained institution.

This creates a domino effect. With federal oversight increasing, fraudulent applications add work to already overwhelmed admissions, IT, and financial aid staff. Instead of preparing to welcome new students, their time is diverted to sifting through enrollment data to figure out if students are even real.

Those that do get past the manual checks steal classroom seats from students who want them and strip financial aid from those who need it. With fewer resources for actual learners, higher education institutions risk eroding trust with students and stakeholders, making degrees out of reach for those who are willing to work for them.

Colleges and universities can get ahead of bad actors using the right tools to help monitor and detect fraud faster with:

- **End-to-end visibility**
- **Proactive defense**
- **Digital resilience**

Nearly $90 million in federal student aid was fraudulently disbursed in 2025, including more than $40 million to fake students.

CHALLENGE 1:

Fragmented systems let fraud slip through the cracks

Higher education institutions run on data and that data lives across vast networks of siloed tools that fit each department's unique needs. Admissions has one tool to track enrollment, financial aid has another to account for funds allocated to specific students, and professors have yet another to input student grades and attendance. Each tool accomplishes necessary tasks, but when siloed, they create disconnected workflows and visibility gaps for fraudsters to exploit.

Every additional system expands the attack surface. When departments don't communicate about potential fraudulent applications, fake students are admitted and scammers win. Unreliable enrollment data makes it harder to identify how many students actually need financial aid, where to allocate resources, and how to plan for the term ahead.

The Solution:

Catching fake students starts with end-to-end visibility across your tools, systems, and networks so that risk doesn't hide between departments.

With a unifying platform that integrates disconnected systems, higher education institutions can eliminate blind spots to stop ghost students from slipping through the gaps between tools. Instead of trying to correlate isolated data points to catch fraud, teams can now work from a shared view of activity across the full student lifecycle.

Once they have unified signals, teams can quickly and confidently cross-verify personal information — such as a student's identity, address, and income — across internal databases, public records, and vendor tools. From there, real-time screening turns every incoming application into a signal you can act on to verify identity and shut down fraud before the institution disburses aid.

Unified visibility also helps streamline your tech stack, reduce tool sprawl, and eliminate technical debt, modernizing institutional systems without adding complexity. And instead of guessing where there might be fraud, college and university staff can start seeing the full fraud spectrum.

FraudWatch, from Conducive Consulting, brings this unified view to life. Built on the Splunk platform, it helps stop fraudulent applications early by verifying applicant information in real time and giving key teams clear visibility into potential risk across the enrollment process.

California community colleges reported losing over $10 million in federal aid and $3 million in state aid to fake students from March 2024–2025.

CHALLENGE 2:

Modern fraud is moving faster than higher education can respond

Fraud tactics have evolved over time. They may have started with bursts of applications sharing the same address, phone number, and email but have quickly turned to coordinated schemes with multiple “students” routing funds to the same bank account.

In higher education, fraud peaks around registration and aid disbursement windows when teams are already slammed. The challenge isn’t just about more fraud — it’s fraud hitting at the worst possible times.

To keep up, security and IT teams must swivel between admissions, financial aid, identity verification, and finance systems, chasing alerts all day without the context to know what’s connected or what matters most. Every system tells part of the story, but none have the whole picture.

This creates both a visibility and staffing problem. Manual review leads to alert fatigue, slow investigations, and a reactive posture that strains the already-stretched teams responsible for keeping higher education systems running and real students moving forward.

The Solution:

The only way to keep up with sophisticated threats and new fraud schemes is to build a resilient, proactive defense. That starts with end-to-end visibility. Continuous monitoring across systems brings fragmented signals together to prioritize detections in real time and with context. Now, you’re adapting with the threat landscape instead of chasing every alert.

To further streamline response, AI-driven anomaly detection can analyze applicant data, IP addresses, and device fingerprints to surface stolen or synthetic identities. Machine learning (ML) goes even further by uncovering hidden patterns to quickly identify anomalies across users, devices, and applications that manual review could miss.

AI-powered tools cut investigation times in half by orchestrating repetitive tasks, accelerating containment, and ensuring consistent response. This allows your admissions and financial aid teams to shift their focus to supporting real students.

As attackers adapt, Conducive’s FraudWatch keeps up. The combination of real-time visibility, AI-driven detection, and automated response helps institutions protect students, safeguard funds, and keep education and financial aid accessible.

More than 62% of education professionals say a lack of cybersecurity staff was very or somewhat stressful.

CHALLENGE 3:

IT teams lack the staff to implement the right systems

In higher education, IT teams are often lean by design, but they're expected to support sprawling environments, critical systems, and thousands of users — all with limited budgets and tight timelines. Add in a threat landscape that's evolving fast and that leaves teams little time for strategic system implementation.

You know how it goes: A new tool requires heavy customization, constant tuning, and specialized knowledge. This adds to your team's to-do list, reducing their capacity and delaying progress. Even with the right tools, limited time and resources can slow deployment, leaving gaps that attackers can quickly exploit.

The Solution:

The right tools paired with the right implementation partner help teams modernize their security posture with confidence. With expert-led implementation, institutions can accelerate ROI on their tool investments and ensure that the capabilities they need are fully operational from the start.

Your technology partner must also understand the realities of higher education IT and cybersecurity — tight budgets, small teams, a large attack surface, and records under federal scrutiny. A partner like Conducive Consulting, with extensive higher education expertise, can design custom solutions for your environment, funding models, and compliance requirements.

In addition to implementation, Conducive helps teams stay current as threats and technology evolve, with continuous training that doesn't disrupt day-to-day operations. The payoff multiplies over time, as teams are able to scale security without complexity.

Proven practices, expert guidance, and easy-to-follow workflows equip small teams to investigate faster, respond quicker, and stay ahead of emerging threats without increasing operational overhead.

48% of public sector security leaders surveyed said their team is understaffed, while another 41% say their team is overworked.

Source: Splunk, State of Security Action Guide for the Public Sector, 2025

Protecting students, funds, and trust

Fraud doesn't live in a single system, and neither should your defense against it. A resilient admissions process requires coordinated action across admissions, financial aid, and IT.

That's where FraudWatch, built by Conducive, comes in. A custom-built tool for higher education, FraudWatch stops false applications before they disrupt higher education enrollment through real-time verification and fraud detection. It not only flags suspicious activity, it also gives teams clear, actionable insights that surface key risk indicators, ensuring a strong security posture.

Built on the Splunk platform, FraudWatch provides:

- End-to-end monitoring that tracks fraud from application to financial aid disbursement.
- Real-time screening to reduce fraud before it enters the enrollment pipeline.
- Multisource data integration to verify applicant information.
- Dashboards and investigative tools that support audits, compliance, and investigations.

With nearly 15 years of Splunk experience, Conducive Consulting offers cost-effective enablement and managed services to help colleges and universities deploy FraudWatch quickly, operate it confidently, and get the most out of their investment without adding strain to their IT teams.

Simplify security and accelerate value with FraudWatch.

FraudWatch©

> "FraudWatch helps us catch fraudulent applications before they reach our admissions staff. It's like having a tireless assistant who never stops learning."
>
> Admissions Director,
> Community College Partner

CONDUCIVE | splunk> a CISCO company

© 2026 Conducive Consulting. All rights reserved.

Splunk, Splunk>, Data-to-Everything, and Turn Data Into Doing are trademarks or registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2026 Splunk LLC. All rights reserved.