LexisNexis®
RISK SOLUTIONS

Higher Education Institutions at Risk

Public community and technical colleges are facing significant fraud risk challenges, particularly in the areas of enrollment and financial aid. These challenges have intensified in recent years, with fraudulent activities becoming more sophisticated and widespread.

Financial Aid Fraud

Financial aid fraud has surged dramatically over the past five years, costing U.S. higher education institutions approximately $100 million per year as of 2023, compared to less than $10 million annually before 2020[1]. In California alone, community colleges lost $7.6 million in aid to fraudulent identities in the first three quarters of 2024, up from $4.4 million in 2023 and $2.1 million in 2022[1].

Ghost Students and Enrollment Fraud

Community colleges are particularly vulnerable to "ghost students" due to their simpler application processes, lower admission standards, and prevalence of online course offerings[2]. Fraudsters exploit these factors to create fake student profiles, enroll in courses, and apply for financial aid. In some cases, they use stolen identities or even those of prison inmates to perpetrate these schemes[2].

Technological Exploitation

The shift to remote learning during the COVID-19 pandemic has exacerbated the fraud risk:

1. **Artificial intelligence (AI)-powered spambots now mimic human behavior**, completing assignments, participating in discussions, and even submitting essays[3].
2. **Fraudsters exploit online learning platforms** and unified application systems to submit multiple fraudulent applications easily[3].
3. **Bots flood course registrations**, preventing legitimate students from enrolling in necessary classes[3].

Impact on Institutions

The consequences of these fraudulent activities are severe:

Financial losses from misallocated aid and increased administrative costs[4].

Disruption of operations and accurate record-keeping[4].

Undermined trust within institutions and from the public[3].

Blocked access for legitimate students to required courses, potentially delaying their academic progress[3].

Countermeasures

Colleges are adopting various strategies to combat fraud:

Implementing AI-driven fraud detection systems have shown promising results in identifying fraudulent applications[3].

Developing internal fraud detection dashboards and manual verification processes[3].

Collaborating with other institutions to share data and insights about fraudulent activities[3].

As the higher education sector becomes increasingly reliant on technology, it must also evolve its fraud prevention strategies to protect both institutional resources and the educational opportunities of genuine students.

LexisNexis® RISK SOLUTIONS

The Attack of Bots

Fraudulent bots mimic human behavior to evade detection by leveraging advanced technologies and techniques that replicate the nuances of real user interactions. Here are the primary methods they use:

1. Behavioral Mimicry

- Bots simulate human-like actions such as mouse movements, typing speeds, swipe patterns, and hover times. This includes replicating the timing and pressure sensitivity of interactions on mobile devices, making them appear indistinguishable from genuine users[5].
- Advanced bots use "behavioral hijacking," where they record and replay real user interactions to create highly realistic activity patterns[6].

2. Use of AI and Machine Learning

- Machine learning algorithms enable bots to learn and adapt human behavioral patterns dynamically. They analyze data from real user interactions and refine their actions to closely match human behavior over time[7].
- Generative models are employed to simulate complex activities, such as navigating web pages or interacting with forms, in ways that mimic authentic human decision-making processes[5].

3. Evasion Techniques

- Bots rotate intellectual property (IP) addresses, switch user-agent strings, and utilize mobile emulators to avoid detection based on device or browser characteristics[8].
- They operate in a "low and slow" manner, spreading activities across different IPs or geolocations to avoid triggering rate-based detection systems[8].

4. Full-Fledged Browser Usage

- Some bots operate within full-fledged browsers, often hijacked by malware, allowing them to interact with websites in ways that closely resemble human users. This includes handling JavaScript execution, cookies, and CAPTCHA challenges[6].

5. Continuous Learning Systems

- Bots employ continuous learning frameworks that collect data from real human interactions (e.g., keystrokes, clicks) and adapt their behavior accordingly. This iterative process ensures they stay ahead of detection systems by mimicking evolving human behaviors[5].

These sophisticated capabilities make advanced bots exceptionally challenging to detect using traditional methods like CAPTCHAs or anomaly-based analytics, necessitating more robust detection systems that incorporate AI-driven behavioral analysis and multi-layered security protocols.

Solutions for Today’s Challenges

Colleges could leverage several advanced tools and systems to combat enrollment fraud:

1. Establish Digital Identity

Leverage crowd-sourced intelligence comprised of web and mobile device identification, digital identity intelligence that includes behavioral analytics and machine learning, and frictionless risk-based authentication.

2. Determine Email Risk

Utilize risk assessment that uses email address as a core identifier. Artificial intelligence and real transaction outcomes combine for a clearer picture of identity risk with an email risk score.

3. Amplify Identity Verification

Verifying an applicant’s identity is critical. It’s also extremely challenging with the rise of mobile channel use, synthetic identities and bot attacks. Identity management authentication should automatically adjust to the threat-level posed by the individual and the transaction.

4. Determine Step-Up Authentication

Deploy an identity orchestration solution like LexisNexis EssentialID™, that incorporates continuous authentication through patented, proprietary analytics to help colleges assess risk and reduce friction for trusted applicants, while stepping up authentication when risk level is high.

These tools and systems represent a multi-layered approach to combating enrollment fraud, combining advanced AI technologies with traditional verification methods and inter-institutional collaboration.

LexisNexis®
RISK SOLUTIONS

Security is essential to higher education institutions and prioritizing a people-first approach while simultaneously preventing cyber threats is critical. Identity security and assurance isn't just a one-time transaction or event. It's ongoing, with a past, present, and future — constantly evolving. It is essential to have a comprehensive, long-term perspective on identity.

LexisNexis EssentialID™ is an award-winning, seamless, and secure identity orchestration platform providing colleges multi-layered, fraud-resistant identity verification, third-party data integration and decision-making capabilities.

Balance Access and Trust

Generate more reliable and actionable outcomes through our **99.99% linking precision rate**.

Protect your college from risk by leveraging our **adherence to strict ethical standards in data use and privacy** and **proven expertise in regulatory compliance**.

LexisNexis® RISK SOLUTIONS

Please contact us today, to see how we can help protect your college.
Tel: 1-800-869-0751

Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global identity verification provider of information-based analytics and decision tools for professional and business customers.

1. Fighting Financial Aid Fraud in Higher Education | EDUCAUSE Review
2. Understanding and Preventing Fraud in Higher Education
3. How AI Is Combating Enrollment Fraud at Community Colleges
4. Colleges and Universities Growing Threat of Bots Stealing Financial Aid or Student Seats - A.M. Simpkins and Associates
5. dsn13-final.dvi
6. How 4th-Gen Bots Are Fooling Fraud Detection
7. Online fraud and the blurred lines between bots and humans | Security Info Watch
8. Threat Spotlight: Bad bots are evolving to become more 'human' | Barracuda Networks Blog