KEEPING HIGHER EDUCATION INSTITUTIONS S.A.F.E. FROM STUDENT FRAUD APPLICATIONS
Keeping Higher Education Institutions S.A.F.E. From Student Fraud Applications

Table of Contents

Introduction ........................................................................................................................................2
Why fraud application is a concern ................................................................................................. 2
Tactics Used by Fraudsters ............................................................................................................... 3

1. Identity Theft .................................................................................................................................. 3
2. Falsifying Transcripts and Test Scores .......................................................................................... 4
3. False Documentation ...................................................................................................................... 4
4. Ghost Students .............................................................................................................................. 4
5. Insider Collusion ............................................................................................................................ 4
6. Multiple Applications ..................................................................................................................... 4
7. Scholarship Scams .......................................................................................................................... 5
8. Bribery ........................................................................................................................................... 5
9. Impersonation ............................................................................................................................... 5
10. Virtual Fraud ................................................................................................................................ 5

Impacts on Higher education institutions ......................................................................................... 5
The solution – S.A.F.E...................................................................................................................... 7
How does S.A.F.E. work? .................................................................................................................... 7

1. Multi-Level Customizable Approach ............................................................................................. 7
2. Fraudulent Verification Process ...................................................................................................... 8
3. Secure Encryption and Revolving Data Keys ................................................................................ 8
4. Customizable Alerts and Notifications ......................................................................................... 8
5. Easy Integration ............................................................................................................................. 8

S.A.F.E. features and benefits ............................................................................................................. 9
Using S.A.F.E. to stop student application fraud .............................................................................. 10
Conclusion .......................................................................................................................................... 10
Introduction

Higher education has long been a pathway to personal and professional success for students. Still, unfortunately, it has also become a prime target for fraudsters seeking to exploit the system for personal gain. In recent years, colleges and universities have increasingly become hot targets for fraud rings and scammers looking to steal as much government funds as possible through student application fraud. The problem is not only a financial burden on higher education institutions but also a significant threat to the integrity of the admissions process and the future of our educational system.

The rise of student application fraud is a complex issue requiring a multifaceted approach. While the problem has existed for decades, technological advances and the internet have made it easier for fraudsters to carry out their schemes. The high demand for college degrees, coupled with the increasing cost of tuition and limited financial aid options, have made obtaining higher education more challenging for students, leading some to resort to fraudulent means to secure funding.

Therefore, student fraud application detection methods such as background checks, verification of academic credentials, and identity verification can help institutions identify and stop fraudulent applications. Institutions that do not have adequate detection and prevention methods in place may unknowingly accept fraudulent applications. Hence, it is essential to explore the growing problem of student application fraud in higher education, including the tactics used by fraudsters, the impact on colleges and universities, and strategies for prevention and detection.

Why fraud application is a concern

California's community college system received over 65,000 fake financial aid applications in 2021. One community college, Chaffey College, identified and stopped approximately $1.7 million in attempted student application fraud. Unfortunately, the San Diego Community College District was only able to identify and stop the fraud after having paid out more than $100,000 to fraudsters.

The financial implications of such student application fraud are significant. Fraudulent applications can lead to colleges and universities disbursing
financial aid to students who are not eligible, or even worse, to non-existent students. They deplete government funds creating a financial burden on the institutions that may have to repay these funds back to the government. Moreover, fraud applications can harm the students who genuinely need the aid, as the limited funds are diverted to those who don't qualify, ultimately affecting the overall financial stability of the higher education system.

Furthermore, student application fraud can damage the reputation of higher education institutions, making them less attractive to legitimate students and reducing the credibility of the degrees they offer. As more fraudulent cases come to light, the public's trust in higher education erodes, creating a ripple effect beyond financial harm.

In light of this, preventing student application fraud should be a priority for higher education institutions. Colleges and universities need to be proactive in implementing effective strategies. Some of these strategies include increased identity verification and background checks, mandatory documentation verification, and fraud detection software. Additionally, educational institutions must work with government agencies and other stakeholders to develop policies and procedures that reduce the opportunities for fraud and strengthen the penalties for those caught committing fraud.

Tactics Used by Fraudsters

1. Identity Theft

Fraudsters often use identity theft to commit student application fraud. They obtain personal information, such as social security numbers, dates of birth, and contact information, from real students and create fake student profiles. They then use this profile to apply for financial aid or enroll in courses. Identity theft is a common tactic used by fraud rings targeting higher education institutions because students are at four times greater risk of becoming identity theft victims. As such, scammers use identity theft to obtain large sums of government funds. Institutions can prevent this tactic by implementing strict identity verification processes, including multi-factor authentication and background checks.
2. Falsifying Transcripts and Test Scores
Fraudsters may falsify academic records to meet eligibility criteria for scholarships, grants, or enrollment requirements. International students are particularly vulnerable to this tactic, as they may not have access to the required documentation or lack the English language skills needed to pass exams. The tactic is concerning because it can result in unqualified students cheating their way into academic programs. Educational institutions need rigorous document verification processes to catch these discrepancies, such as requiring official transcripts or test scores directly from the issuing organizations.

3. False Documentation
Criminals may submit false documentation to meet financial aid or enrollment eligibility criteria. They may use software or photo editing tools to create convincing-looking documents. Institutions need to verify the authenticity of these documents by requesting original or certified copies, comparing them to government records, and checking for inconsistencies.

4. Ghost Students
Fraudsters create fictitious students, commonly called "ghost students," by fabricating a name, address, social security number, and other details to receive financial aid payments. Because no actual student is attending classes, this tactic is difficult to detect, as was the case in California in 2021. Higher Education institutions need to also consider other hidden costs, such as, hiring more professors to manage seat capacity for phantom seats and for scammers robbing these seats from real students can add significant costs to an institution over time. Educational institutions can mitigate this risk by regularly auditing student records and verifying enrollment status with professors.

5. Insider Collusion
Scammers may bribe or collude with insiders in higher education institutions, such as admissions officers or financial aid counselors, to manipulate the application process in their favor. This tactic can be difficult to detect, but instituting a whistleblower policy and conducting regular background checks can help reduce the risk.
6. Multiple Applications
Fraudsters may submit multiple applications using different names and social security numbers to receive financial aid multiple times. Fraudsters are also using advanced technology like bots to submit hundreds of applications at a time for penetration testing. Educational institutions can use software to detect duplicate applications, preferably in real-time, or require that students submit applications through a centralized system that has fraud prevention protocols in place.

7. Scholarship Scams
Fraudsters create fake scholarship opportunities that require students to pay an upfront fee or provide personal information, then disappear with the money or use the information for identity theft. Students should only apply for scholarships from reputable organizations and never provide personal information or pay upfront fees to avoid these scams.

8. Bribery
Fraudsters may offer to bribe officials to overlook application discrepancies or receive preferential admissions treatment. Educational institutions should have strict policies against accepting bribes and conduct regular ethics training for staff members.

9. Impersonation
Fraudsters may impersonate a college or university representative to solicit sensitive information or to offer fraudulent financial aid or enrollment opportunities. Students should be wary of unsolicited emails or phone calls and verify the institution's legitimacy before providing any personal information.

10. Virtual Fraud
Fraudsters may use the internet to create fake websites or social media accounts that mimic legitimate colleges and universities to scam students out of money, personal information, or acceptance into the institution. Students should verify the legitimacy of the website or social media account by checking for the institution's official seal or logo and contacting the institution directly.
Impacts on Higher education institutions

Compliance risks are a significant concern for institutions, as non-compliance with federal regulations can result in fines and penalties. Higher education institutions must comply with numerous regulations, including the Higher Education Act and Title IV regulations, which govern the distribution of federal financial aid. Compliance personnel must monitor and enforce these regulations, which can be complex and time-consuming. Failure to comply can result in significant fines and harm to the institution's reputation.

Fraudulent activity can also impact student diversity, as fraudsters may manipulate applications to obtain financial aid or admission, resulting in fewer opportunities for underrepresented and marginalized students. As a result, this can have significant long-term consequences for society, as a lack of diversity in higher education can limit access to new perspectives and ideas. Institutions must strive to provide equal access to education and ensure that their admissions processes are fraud-free to promote diversity and inclusivity.

In addition, fraudulent activity can also lead to demoralization among faculty, staff, and administrators. These individuals work tirelessly to uphold academic integrity, and fraud can undermine their efforts. Subsequently, this can lead to decreased morale, job dissatisfaction, and even burnout. Institutions must invest in training and resources to enable staff to effectively detect and prevent fraudulent activity while promoting a positive work environment.

Furthermore, preventing and detecting fraudulent activity requires significant effort and resources from institution staff, including admissions officers, financial aid officers, and compliance personnel. As a result, this can lead to increased workload and job stress, affecting job satisfaction and retention. Institutions must invest in training and technology to enable staff to effectively detect and prevent fraudulent activity while promoting a positive work environment.

Fraudulent activity can also strain student-faculty relationships. Unqualified students admitted through fraudulent means may struggle to keep up with academic demands, resulting in frustration and disappointment among faculty. It can impact the learning environment and overall student experience. Institutions must work to maintain the integrity of academic programs and
ensure that students admitted are qualified and capable of completing the program.

Finally, fraudulent activity can have significant legal consequences for institutions. Institutions that fail to prevent or detect fraudulent activity may face legal liability from affected parties. The parties include students who were denied admission or financial aid due to limited resources and may feel that they were unfairly excluded due to fraudulent activity. Institutions must have effective policies and procedures to prevent and detect fraudulent activity while protecting themselves from legal liability.

The solution – S.A.F.E.

AMSA's S.A.F.E. application is a comprehensive solution designed to aid higher institutions in preventing fraudulent and suspicious activity at the source. S.A.F.E. uses a verification process that employs multiple checks across the institution's data and against S.A.F.E.'s data broker network. The checks examine several data points in each application record to identify and reject fraudulent applications. Furthermore, S.A.F.E. acknowledges the unique nature of each institution's business rules and processes and offers a multi-level customizable approach that incorporates additional layers of detection. This feature provides greater insight into application data to protect institutional assets from scams and fraudulent activity.

AMSA's S.A.F.E. application has a built-in fraudulent verification process that uses the organization's proprietary A.I. and Machine Learning processing. This process identifies and classifies every fraudulent application attempt with accuracy. With the help of A.I. technologies, the verification process cuts through the noise of daily alerts and provides rapid insights that minimize response time. Additionally, S.A.F.E. employs secure encryption (in transit/at rest) and revolving data keys to safeguard institutional data at every stage of the verification process. Overall, AMSA's S.A.F.E. application is a flexible and dependable solution that empowers higher ed institutions to shield their assets from fraudulent activity and maintain the integrity of their admissions process.
How does S.A.F.E. work?

1. Multi-Level Customizable Approach
S.A.F.E. provides a multi-level customizable approach that offers additional layers of detection to protect institutional assets from fraudulent activity. This approach takes into account that each institution has specific business rules and processes to consider. By offering a customizable approach, S.A.F.E. provides deeper insights into application data to fortify efforts to protect against scammers and fraudulent activity. Institutions can set their risk thresholds, determine the level of risk they are willing to accept and strike a balance between protecting their assets and ensuring that they don't reject legitimate applications incorrectly. This customizable approach offers flexibility to institutions, allowing them to adjust the solution according to their unique needs and circumstances.

2. Fraudulent Verification Process
S.A.F.E. offers a built-in fraudulent verification process that uses AMSA's proprietary A.I. and machine learning processing. The system identifies and classifies each fraudulent application attempt, providing rapid insights that drastically reduce response time. The machine learning algorithms adapt to evolving fraud trends, enabling the system to identify and prevent fraudulent activity with greater precision. With advanced technologies, the verification process cuts through the noise of daily alerts. It provides real-time alerts and notifications to inform institutions about suspicious or fraudulent activity.

3. Secure Encryption and Revolving Data Keys
S.A.F.E. provides multiple levels of security when working with institutional data. The solution employs secure encryption (in transit/at rest) and revolving data keys to protect every piece of data. This feature ensures that institutional data is always secure, no matter what stage of the verification process. S.A.F.E. solution integrates seamlessly with existing institutional systems, making implementation simple and stress-free.

4. Customizable Alerts and Notifications
S.A.F.E.'s real-time alerts and notifications help institutions stay informed about fraudulent activity. These alerts can be customized to suit the specific needs of each institution, ensuring that relevant stakeholders are kept up-to-date at all
times. Institutions can set their alerts and notifications, determining the frequency and format of the alerts they receive. This feature provides peace of mind, knowing institutions are always informed about suspicious or fraudulent activity.

5. Easy Integration
S.A.F.E.'s solution integrates seamlessly with existing institutional systems, making implementation simple and stress-free. Depending on the preferences, institutions can deploy the solution in the cloud or on-premise. Institutions can choose the deployment method that best suits their needs, making the implementation process smooth and straightforward.

S.A.F.E. features and benefits
S.A.F.E. (Student Application Fraudulent Examination) offers a variety of cybersecurity features that can help higher institutions to prevent fraudulent and suspicious activity at its origin. One of the most significant features of S.A.F.E. is its enhanced due diligence capability. This feature begins with a series of checks across the data using multiple data points of each application record to determine whether it is a fraudulent attempt. S.A.F.E. analyzes the I.P. location, phone number, email address, and type of activities of the applicant to identify any suspicious or fraudulent behavior. This feature also collects demographic data, such as frequency, to provide deeper insights into the applicant's behavior and to fortify the institution's efforts to protect institutional assets from being vulnerable to scammers or fraudulent activity.

Another crucial feature of S.A.F.E. is its identity verification process. This feature verifies the identity of each applicant before granting admission into the institution. S.A.F.E. collects the applicant's name, date of birth, address, and identification number (such as Social Security Number) to ensure they are who they claim. As such, this helps to eliminate the risk of fraud and identity theft, which is especially important for higher institutions that deal with sensitive information.

S.A.F.E. also offers advanced reporting and analytics capabilities that allow institutions to gain insights into suspicious activity. This feature includes geographic location, activity type, suspicion level, and custom reports. With this feature, institutions can track and monitor suspicious activity, allowing
them to take action quickly and efficiently. Generating custom reports is particularly helpful, allowing institutions to focus on the metrics most relevant to their business.

The ongoing monitoring feature of S.A.F.E. allows institutions to track and monitor suspicious activity in real time. This feature detects spikes in activities, out-of-area or unusual cross-border activities, and the inclusion of people on sanction lists. Ongoing monitoring is particularly important for higher institutions, as it lets them quickly detect and prevent fraudulent activity before it becomes a major issue.

**Using S.A.F.E. to stop student application fraud**

S.A.F.E. is a multifaceted tool that utilizes artificial intelligence and machine learning algorithms to identify and flag suspicious patterns in student applications. It analyzes data from various sources, including academic records, personal information, and behavioral patterns, to identify any inconsistencies or discrepancies that may indicate fraudulent activity. By leveraging S.A.F.E., educational institutions can streamline their admission processes, minimize the risk of accepting fraudulent applications, and ensure the quality of education offered. This solution is a powerful tool for EdTech, colleges and universities, application management systems, CRM systems, and software companies, all of which can benefit from its advanced features.

S.A.F.E. is incredibly user-friendly and can be seamlessly integrated with existing software solutions, making it an accessible solution for educational institutions of all sizes. By adopting S.A.F.E., institutions can boost their security, S.A.F.E. guard their reputation, and prevent financial losses caused by fraudulent activities. S.A.F.E. is a valuable investment for any educational institution looking to maintain the integrity of its admission processes and ensure the quality of education they provide.

The benefits of using S.A.F.E. extend beyond preventing fraud. This solution can also help institutions improve the overall quality of their student body by ensuring that they admit only qualified students. By streamlining the admission process and reducing the risk of fraudulent activity, S.A.F.E. can also help institutions enhance their reputation and attract more qualified applicants.
Furthermore, S.A.F.E. is an adaptable solution each institution can tailor to its business processes and operations. Its advanced features allow institutions to customize the fraud detection process and prioritize the most critical aspects of their admissions process. Additionally, S.A.F.E. can be seamlessly integrated with existing software solutions, making it a user-friendly and accessible solution for educational institutions of all sizes.

**Conclusion**

The issue of fraud in student applications is a growing concern for educational institutions worldwide. With the rise of digital technology and online application processes, it has become easier for individuals to submit falsified information and documents, resulting in admissions decisions not based on merit or genuine qualifications.

To prevent this problem, institutions must implement effective fraud prevention strategies and utilize advanced technologies to detect fraudulent applications. These strategies should include data analytics, artificial intelligence, and machine learning to identify fraud patterns and anomalies in application materials.

In addition, educational institutions should prioritize verifying the authenticity of application documents and conducting thorough background checks on applicants. They can achieve this through partnerships with external verification agencies and secure online platforms for document submission.

Ultimately, preventing fraud in student applications is crucial for maintaining the integrity of the educational system and ensuring that deserving students get the opportunity to succeed. By adopting a proactive and comprehensive approach to fraud prevention, institutions can safeguard their admissions processes and protect the value of their degrees.