Fighting Student Loan Fraud with Okta and LexisNexis® RiskSolutions

Help decrease fraud and improve productivity by verifying student identities and automating college account creation

Higher education institutions have seen an increase in funding and online classes, leading to a spike in student loan and grant fraud cases. Fraudsters have been taking advantage of stolen identities, leaving institutions unable to cope with the scale and complexity of these attacks.

The disconnected nature of higher education systems isn't helping either since fraudsters can easily use IDs stolen from one college to defraud another, and even from state to state, without fear of being caught.

Student loan and grant fraud are currently costing taxpayers hundreds of millions of dollars each year. But, used together, Okta and LexisNexis® Risk Solutions can help mitigate student loans from being issued to fake, fraudulent, or synthetic students through secure and powerful identity verification and access management services, all with minimal user friction.

How fraudsters are stealing student aid

One of the ways fraudsters are taking advantage of outdated systems in higher education is by registering fake students for classes. Online classes are the biggest target. Class seats are taken up by fake students, blocking access to legitimate students, and fraudsters receive the aid these fake students appear eligible for. These fake students can also make it look like classes that wouldn't otherwise meet the minimum student requirement are large enough to run. Schools are left with two poor options when this happens: cancel the class after removing the fake students or continue the class and lose money.

> *California's community college system seeks $100 million in technology and security upgrades after several fraud instances. The fraudsters used bots to create 60,000 aid applications from fake student accounts. This, coupled with abnormal enrollment patterns on community college research lists, pointed faculty and administrators toward a bot attack and the need for security upgrades.*

Current solutions often require professors and administrators to vet whether students are legitimate. This takes up professors' time and requires training on spotting fake students and reporting to administration. Some college systems are asking faculty to contact each student individually to determine whether they're fake, adding to the teacher workload. Additionally, college administrations now need to report attempted fraud to the state administration, putting additional responsibility on staff and draining school resources.

In the end, institutions are addressing competing challenges. They must address declining enrollment by incentivizing potential students to apply and register for courses. Then, as bad actors apply to institutions, register for courses they will never participate in, and receive financial aid dollars intended for legitimate students, institutions are charged with finding and removing them from their systems. In many cases, enrollment and course registration targets are impacted, and stolen financial aid dollars must be reimbursed by the institutions. These scenarios are faced daily, creating the need to find a way to regain control of the system to make the college experience more secure and streamlined for everyone involved.

The solution to fight fraud

States and educational institutions have the power to mitigate student loan fraud in our higher education system with the help from Okta and LexisNexis® Risk Solutions.

Sensitive data for over 2.5 million individuals with student loans from Oklahoma Student Loan Authority (OSLA) and EdFinancial was exposed after hackers breached the systems of one of their technology service providers.

LexisNexis® Risk Solutions student ID verification and Okta's Identity access and management services effectively work together through existing integrations by:

- Providing robust identity proofing through LexisNexis® Risk Solutions that:
  - Electronically verifies the applicant data and the legitimacy of the provided credential using a scanned copy of the applicant's government-issued ID and comparing it to a picture of the applicant, which will be automatically compared just to the picture on that ID
  - Leverages outside, comprehensive national data on the applicant
  - Augments identities and facilitates risked-based decision-making with additional information, such as whether an individual is currently imprisoned, undocumented, deceased, unbanked, unlikely of age, etc., will only strengthen the overall system to assume those in need truly get access and improve the blocking of fraudulent attempts
- Providing strong and ongoing account management services through Okta's identity and access management services that:
  - Manages identities and access from the cloud, freeing your faculty to focus on student services
  - Ensures each student is the same person who was originally verified with strong yet simple multi-factor authentication or adaptive multi-factor authentication
  - Protects institutions from credential stuffing, botnets, and brute force and DDoS attacks by detecting and automatically acting to shut down bot attacks

How Okta and LexisNexis® Risk Solutions work together

The Okta Identity Cloud brings student data together into a single, powerful digital hub for secure identity management. LexisNexis® Risk Solutions matches records submitted in applications with its national database of billions of verified records and identities to determine whether the application is likely credible and legitimate. The LexisNexis® Risk Solutions system matches records of users as they move through life and change over time, giving a complete and precise picture of a person rather than a single snapshot. Records are then resolved to a single identity to help with tracking over time.

Together, Okta and LexisNexis® Risk Solutions make verifying student identities simple and automatic, taking pressure off valuable faculty and administration so they can focus on their work. Student aid fraud is a national problem that we can fight at the state level.

Managing student identity with Okta and LexisNexis® Risk Solutions can help mitigate major losses, free up faculty, and avoid student aid drain. Visit okta.com/education and risk.lexisnexis.com/GovFraud to learn more.

A Jacksonville man used the identities of family members, drug addicts, and homeless people to steal nearly $300,000 in federal student aid funds. He used false information and fabricated documents on the FAFSA. After enrolling the fake students in Cape Fear Community College, he withdrew them to get refunds from the school.

Okta makes no representations, warranties, or other assurances regarding the content of this data sheet. Information regarding Okta's contractual assurances to its customers can be found at okta.com/agreements. Any statements regarding LexisNexis® Risk Solutions are not representations made by Okta. Okta does not endorse any particular vendor, product or service, and disclaims all warranties, expressed or implied, with respect to LexisNexis® Risk Solutions, including any warranties of merchantability or fitness for a particular purpose.

Thank you for downloading this Okta resource! Carahsoft is the distributor for Okta solutions.

To learn how to take the next step toward acquiring Okta solutions, please check out the following resources and information:

For additional resources:
carah.io/oktaresources

For upcoming events:
carah.io/oktaevents

For additional Infoblox solutions:
carah.io/oktasolutions

For additional Cybersecurity certified solutions:
carah.io/cybersolutions

To set up a meeting:
okta@carahsoft.com
(833)-674-3990

To purchase, check out the contract vehicles available for procurement:
carah.io/oktacontracts