A **CENTER FOR DIGITAL EDUCATION** THOUGHT LEADERSHIP PAPER

Modernizing Identity in Higher Education

A real-world look at fraud risks and identity verification challenges in colleges and universities

SPONSORED BY Socure™

Higher education institutions may not be doing enough to protect digital identities as they move more academic and administrative services online.

This issue came to the forefront in a national survey conducted by the Center for Digital Education (CDE) on digital identity practices in higher education. The research collected responses from 74 higher education officials in September 2024.

We asked leaders how they apply digital identity verification, which technologies and techniques they use, and where they encounter the biggest challenges. An analysis of our findings underscores the reality that many colleges and universities are ill-equipped to confront modern identity threats.

The State of Identity on Campus

Our research and analysis points toward one central takeaway: Higher education leaders should do more to fight identity fraud.

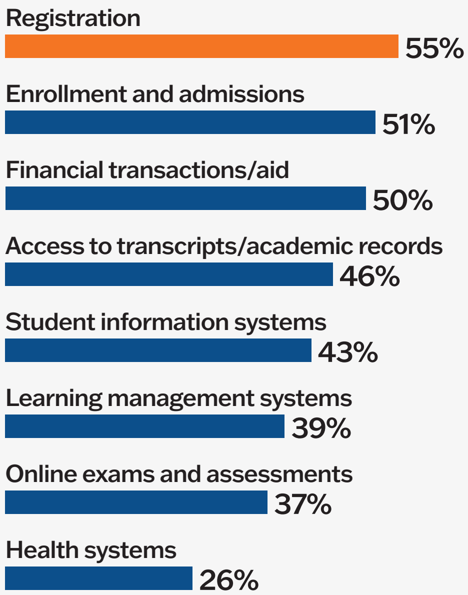
Institutions often struggle to balance online user experience, academic freedom and fraud protection, says Lydia Payne-Johnson, a CDE senior fellow and director of data governance, compliance and identity management at George Washington University in Washington, D.C. In a competitive higher education environment, user experience may get more attention than fraud mitigation.

“If you have a bad student experience at GW, you might just pick up and go over to Georgetown. We don’t want that,” Payne-Johnson says.

Yet, higher education is a target-rich environment for fraudsters. Universities issue email accounts to alumni that may go unused for years. Scammers exploit these accounts to build synthetic identities. Parents and students often use outdated and potentially vulnerable verification techniques to access campus systems and make payments. These issues heighten the need for modern identity protection and fraud-fighting tools.

“Higher ed needs to do quite a bit of work to catch up,” says Payne-Johnson, who formerly worked in the financial sector, where advanced identity authentication and anti-fraud tools are commonplace.

Processes and services where institutions are most likely to apply digital identity verification



Respondents selected all options that apply.

Only about half of CDE survey respondents said their institutions use digital identity verification for crucial processes like registration, enrollment and admissions, and financial transactions. The percentages are even lower for core functions such as learning management systems, online exams and student health systems.

In addition, institutions often use labor-intensive monitoring and manual document reviews to spot fraudulent enrollment activities. These methods are insufficient in a rapidly evolving threat environment, according to CDE Director Brian Cohen. “The risks grow every single day because the bad actors are getting smarter and much more creative,” he says.

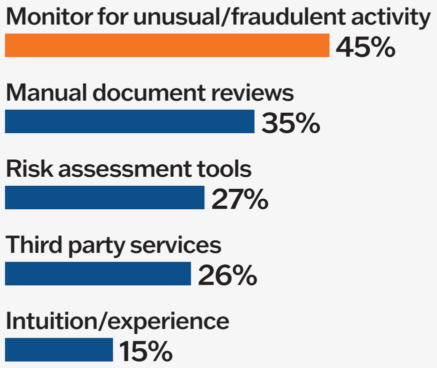
Unused alumni email accounts and weak identity practices are fueling growth of a new threat known as “ghost students,” which are synthetic identities created to bilk institutions out of student loan and government grant funds.

“Fraudsters will use college EDU accounts to perpetuate additional schemes because EDU domains are seen as trustworthy,” says Jordan Burris, public sector general manager with Socure, a leading provider of identity solutions. “We’ve seen in California community colleges that around 20% of enrollment and financial aid applications were fraudulent.”

More than half of survey respondents (53%) said they use more than one identity verification method, and more than a fifth (21%) said they use three or more methods, reflecting the complexities of identity verification. In addition, campuses may rely on legacy identity methods that are ineffective or difficult to use. For instance, almost 30% use knowledge-based authentication (KBA), where users answer security questions. KBA has become far less effective because cybercriminals often have access to users’ personal information through stolen data or publicly available social media accounts.

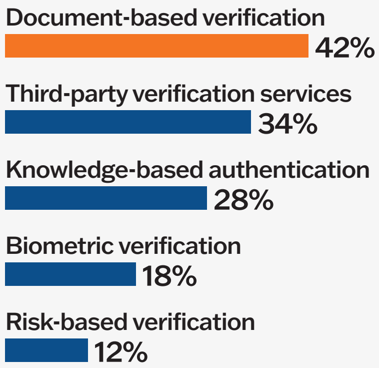
On the other hand, risk-based verification — one of the most promising defenses against advanced tactics like ghost students — was used by just 12% of survey respondents. Risk-based applications examine the context of a user attempting to be authenticated. The applications start with personal data like names, emails,

Most common tactics for detecting identity-related security threats during student enrollment



Respondents selected all options that apply.

Most common digital identity verification methods in higher education



Respondents selected all options that apply.

addresses and birth dates. They also assess data from users' devices such as software and browser versions. AI algorithms calculate a risk score by comparing this real-time, contextual data to a massive database of known fraud behaviors. This process dramatically improves verification outcomes.

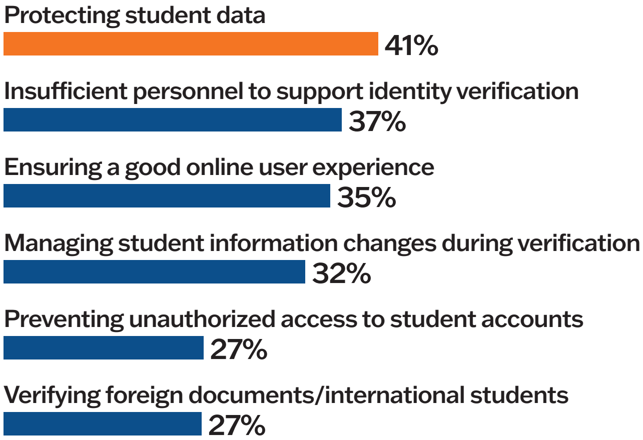
"We've purpose-built our platform to analyze fraud patterns and provide a response in less than a second," Burris says. Most legitimate users are quickly approved. Users whose data raises questions may need to provide government-approved documentation like a driver's license or passport.

Greater use of automation and risk-based verification methods helps institutions strengthen data protection, reduce pressure on internal staff and improve online user experience — all of which ranked as top identity challenges for higher education leaders.

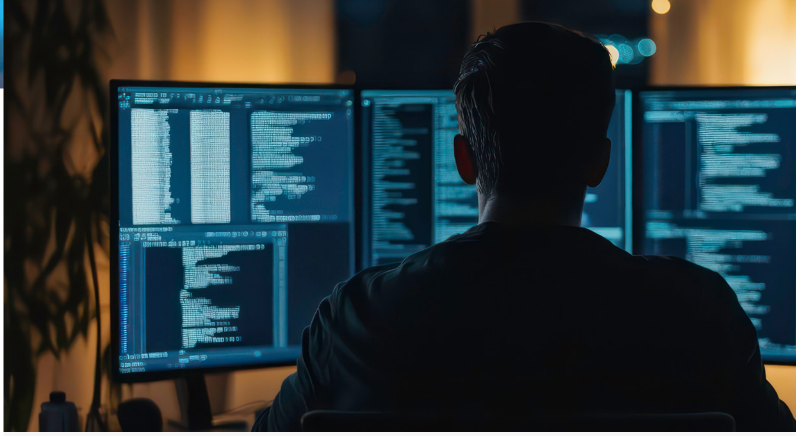
Modern identity verification solutions are also more inclusive than traditional methods, an important consideration for higher education institutions. "Students may not have a long credit history to verify identity," Cohen says.

Burris concurs: "More than 20% of the U.S. population is credit invisible." Legacy identity methodologies can lock these students out of online enrollment systems, creating another barrier for marginalized or low-income groups that already have a harder time getting into college.

Top student identity challenges for institutions



Respondents selected up to five answers.



Identity Theft on Campus

College campuses are fertile ground for identity thieves. Jim Jorstad, a CDE senior fellow and former CIO at the University of Wisconsin-La Crosse, has seen his share of identity vulnerabilities.

From first-year undergrads to retirees, members of campus communities often use passwords that are easy to guess. They also share passwords and logins. And they're vulnerable to social engineering scams.

"Faculty and staff are notorious for clicking on links," Jorstad says. The link might set ransomware in motion or connect them to sophisticated fraudsters who talk them into handing over login or bank account information. Among the more unnerving threats are disgruntled employees who cash in on their insider status and sell valuable data to fraudsters.

Not all fraud is digital, however. Criminals will sneak into dorm buildings, walk into unlocked rooms and grab documents containing personal information. They'll even dig through trash for vital data.

Jorstad recalls going on a dumpster-diving mission during his CIO days to see how serious the problem was. "People threw a bunch of documentation in the dumpster," he says. "When I went out there, it was filled with Social Security numbers and salary information — all on top of the bin."

How can campuses fight identify fraud? "It all comes down to training," Jorstad says. Everyone needs consistent, continuous guidance on:

- ☑ Keeping documents with vital data out of sight
- ☑ Protecting online accounts with strong passwords and never sharing ID credentials
- ☑ Shredding sensitive documents
- ☑ Avoiding links from unknown sources
- ☑ Understanding how fraudsters exploit trust

The Case for Modernizing Digital Identity

GW's Payne-Johnson says higher education officials are awakening to identity threats.

"They need to be able to validate students, faculty, staff — people calling in not just locally, but from around the world — and they need the right tools to monitor this activity," she says.

Here are the biggest benefits of modernizing your institution's digital identification technologies and processes.

Reduced staff workload and improved efficiency. Higher education IT teams don't have enough bandwidth or experience to stop determined, pervasive fraudsters. Here's a familiar scenario: A fraudster checks your LinkedIn profile, sees where you went to college and correctly guesses the email address to your alumni account, which you haven't used in years. They call the university's help desk and ask for a password reset. The help desk agent, who has no effective way of validating the caller's identity, resets the password and the scammer gets in.

Modern identity platforms use AI to assess identity fraud risk in real time, allowing most transactions to be conducted safely and effectively with less load on university staff.

Better user experience. Fast, accurate and friction-free identity verification is a differentiator in an environment where institutions often compete for students and faculty talent.

"Faculty do not like fraud prevention if it affects their ability to do their job efficiently and effectively," says Jim Jorstad, a CDE senior fellow and former CIO at the University of Wisconsin-La Crosse.

Socure's Burris says cumbersome identity processes impose a time tax on users. Modernization offers a tax cut. Instead of taking hours or days, approvals happen in less than a second for most users. Even complex cases are settled faster because modern platforms automate multiple manual processes.

Evaluating Solution Capabilities

Modern identity verification and anti-fraud solutions provide a great user experience while validating identity documents, detecting fraudulent behavior and assessing risk.

Look for these features and tools when modernizing identity and anti-fraud systems:

- ☑ AI and other advanced automations that analyze every user in real time; assess the validity of their data and devices; apply a fraud-risk score; and recommend approving, denying or escalating transactions in milliseconds.
- ☑ Integrations with existing technologies and monitoring systems.
- ☑ Multifactor authentication and single sign-on.
- ☑ Biometrics and liveness confirmation.

"All of these tools can and should be used simultaneously — whatever works for your campus the best," says Jorstad.

Stronger security. Fraudsters often develop highly specialized skills. Scammers creating ghost students, for instance, might team up with creators who use generative AI to produce deepfake videos that are almost impossible to distinguish from the real thing.

Deepfakes can fool legacy identity verification processes. An injection attack, for instance, inserts fake video data into the bit stream connecting a user to a verification system. Stopping this kind of attack requires "liveness" algorithms that use the camera on a phone, laptop or desktop to prove a user is a real person.

Modern identity solutions combine liveness checks with risk-based identity verification to protect against fraud and deepfakes. Socure's technology is part of an identity layer that sits between login and approval processes. An online enrollment form gathers private student data like address, birthdate and Social Security number. When the applicant hits the "submit" button, an application programming interface (API) transmits the data to Socure's risk-scoring platform, which assesses the likelihood that the user is authentic and then recommends either approving or denying the transaction. This procedure communicates with other processes like biometric fingerprint scans and liveness checks. This layered approach provides the most robust defense against identity fraud.

Reputation protection. When data breaches or identity thefts appear in the news media, the people who hold the purse strings — like parents and grant funders — take notice.

"Organizations like the National Science Foundation are looking at audit reports," says CDE's Cohen. If audits reveal inattention to cybersecurity or identity protection, grant-funding organizations might send their dollars elsewhere. Lack of modern security and identity tools can also make it difficult for institutions to get cybersecurity insurance.

A college or university builds value by nurturing openness and academic inquiry. Successfully preparing young people for productive careers builds trust and prestige. Criminals exploit these qualities without a second thought. These risks oblige institutions to defend themselves with modern identity and anti-fraud tools.

Identity Modernization Best Practices

These tips will help institutions modernize identity practices and avoid common pitfalls.

Create an identity strategy. A strong plan keeps modernization on track. Prudent planning includes:

- **Measurement.** You'll need reliable data to identify weak points, track fraudsters' behaviors, monitor costs and ensure return on investment.
- **Technology inventory.** Account for all existing identity and anti-fraud tools and assess how new tools fit into your overall IT ecosystem.
- **Stakeholder engagement.** Reach out to executives, academic leaders and administrative users to explain the value of modernizing. Business users in human resources, finance and enrollment should be part of the conversation.
- **Data governance.** Define guardrails for data locations, varieties (structured versus unstructured), user permissions, backup/recovery and Zero-Trust principles.
- **Transparency.** Keep stakeholders informed of project timelines and progress.
- **Change management.** Training people and overcoming resistance to change will be crucial throughout the project.
- **Integrations.** Map how you'll connect new tools with your existing IT environment. Include APIs and on-premises and cloud-based components of your infrastructure.
- **Layered identity.** Identity verification technologies typically operate as layers between data collection processes. For instance, when a student enrolls online, identity layers verify processes for creating accounts and authenticating transactions. Layering ensures that granting access and approving transactions are not one-time checkoffs. They happen

continuously throughout user journeys to keep them secure and private. Biometrics and liveness checking are additional technology layers that make a fraudster's job more difficult.

Focus on UX. Prioritize the user experience from beginning to end:

- **Optimize speed.** AI and automation can help authorize users in less than a second. Seek every opportunity to remove friction and accelerate approvals.
- **Be inclusive.** Remember that first-generation students and marginalized populations pose verification challenges. Don't leave them out.
- **Retire your security questions.** De-emphasize KBA, which has multiple security and usability flaws.
- **Collect feedback.** Survey users to see what's working and what needs improvement. Use analytics data to identify bottlenecks and remove friction.

Start with pilots. Take an incremental, data-driven approach that monitors performance and documents effectiveness.

- **Keep it simple.** Don't overdo things in the beginning. Start with simple pilot projects and iterate based on user feedback.
- **Get advice.** If you're not sure what to pilot, talk to professional colleagues and ask vendors how other institutions have started.

Focus on the future. New threats keep emerging, and new technologies will rise to meet them. Continuously invest in staff training, security testing, and adapting to new risks and opportunities.

Campus Communities Need More Protection

Our research suggests many colleges and universities aren't doing enough to fight fraud and protect identities. The first step toward improvement is acknowledging changes driven by the digital era. "Schools are now more like banks because most of their transactions are online," says CDE's Payne-Johnson.

To fight fraud and protect data, colleges and universities need to adopt identity best practices.

"It's extremely important to know what's going on outside of higher education," says CDE's Cohen. "We can learn from healthcare, finance, government, manufacturing and other industries that have more experience and in some cases more resources."

Emerging tools strengthened by AI and advanced behavioral analysis can plug crucial gaps in identity protection programs. Learning from other industries, building the right partnerships and adopting advanced solutions are essential to modernizing identity across higher education.

This piece was written and produced by the Center for Digital Education Content Studio, with information and input from Socure.

Produced by the Center for Digital Education

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century.
www.centerdigitaled.com

Sponsored by Socure

Socure is the leading provider of digital identity verification and fraud solutions. Its mission is to verify 100% of good identities in real time and end identity fraud on the internet. Socure's platform applies artificial intelligence and machine learning techniques with trusted online/offline data intelligence from physical government-issued documents as well as email, phone, address, IP, device, velocity, date of birth, SSN and the broader internet to verify identities in real time. The company has more than 1,500 customers across the financial services, government, gaming, healthcare, telecom and e-commerce industries.

socure.com

ADOBESTOCK/AI GENERATED