

SECURITY MANAGEMENT

MARCH 2015

A PUBLICATION OF ASIS INTERNATIONAL

Issue & Beyond

× *Big Data*

Leveraging millions of data points during disasters.

× *Terrorism*

Experts assess the potential threats from lone wolves.

×46

CRIME PREVENTION

×54

EXECUTIVE PROTECTION

×60

HEALTHCARE

×36

FITNESS FOR
DUTY



PHOTO BY THINKSTOCK.COM

PASSING THE BIOMETRICS TEST

OHIO'S FIRST COMMUNITY COLLEGE EMBRACES A NEW METHOD OF VERIFICATION FOR ONLINE TRANSACTIONS TO PREVENT FRAUD AND MAINTAIN COMPLIANCE WITH FEDERAL REGULATIONS. **BY MEGAN GATES**

IT'S LATE IN THE EVENING, and after a long day of lectures and office hours, a professor checks the latest discussion posts of her online classes on Blackboard (an online learning management system). But just before she logs off, she notices something odd. Eight students have posted almost identical answers to her questions.

After some digging through the previous weeks' coursework, she notices increased similarities in all of the eight students' work for the semester. She flags the students and, following protocol, notifies the financial aid department. An investigation is launched. The probe reveals that one student had enrolled at the community college under eight different names, using a transcript signed by a nonexistent high school principal. The

individual posing as the student then took out numerous student loans.

With online classes now a standard feature at community colleges and universities across the United States, many in education are beginning to recognize the need for foolproof methods of student verification to make it harder for individuals to engage in fraudulent behavior. Cuyahoga Community College (Tri-C) in northeast Ohio, where those eight identical



students were enrolled, is one of those institutions.

With its six campuses, Tri-C educates almost 52,000 credit and

noncredit students annually, and one-third of these students are enrolled in at least one online class per semester. This means that verification is an absolute must to ensure that students are who they say they are. However, Tri-C found that its verification methods were not sufficient to keep up with its move to online education.

"The community college mission has always been about access, and we do everything we can to provide access to populations that might not normally have access to higher education," says Charles Dull, assistant dean for e-learning and innovation at Tri-C. "We took a very open approach—not thinking folks would want to try to steal from a community college."

That open approach consists of human recognition. When an individual notices something suspicious in a

student's file, they report it up the chain of command. Tri-C also uses a notification system, which checks to make sure that students who are enrolled in online classes have logged in to Blackboard to participate in their classes. But it doesn't check to make sure that students are who they say they are, making it easy for someone to pose as another student by obtaining his or her password and login information for Blackboard.

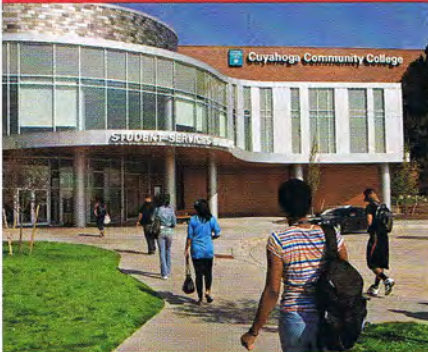
This can be especially problematic if someone is engaging in student loan fraud by enrolling in classes, applying for financial aid and loans, and then dropping the class and pocketing the money with no intention of repaying it.

Along with concerns about fraudulent behavior, Dull was also worried about new federal regulations that would require colleges to do more for student verification than use logins and passwords for online interactions. "I had been reading government reports that were talking about student authentication becoming a requirement for compliance," Dull explains. "And the rule coming out of the Department of Education was that students' login and password weren't sufficient to meet the standards for authenticating a student's identity."

With these concerns in mind, Tri-C decided it needed a new way to verify students from their first interaction online with the college. In 2012, a group of faculty members at a conference discovered a biometric signature product called BioSig-ID. It works by having users handwrite letters or numbers in a confined space by using their finger, mouse, or stylus three times. BioSig-ID then measures the length, angle, speed, height, and number of strokes used to make each character and stores the information in an encrypted database.

Software algorithms then compare this data against patterns collected during the user's subsequent logins, confirming whether they match or not. If they don't match, the user's profile is flagged and sent to an administrator, along with a notice indicating the probability that the attempt is fraudulent, and the user is blocked from accessing the profile.

! STATS



Cuyahoga Community College

Opened
1963 as Ohio's first community college

Has
Six campuses

Serves
52,000 credit and noncredit students annually

Offers
800 distance learning courses;
130 location courses

"We wanted a tool that wasn't going to just say, 'hey, this is fraud; get rid of this student,' but could give us a range of probability from which we could develop a policy," Dull says. "We needed easily readable reports that allow us to make a decision—not just take what came out as black or white." This is especially important as it ensures that students who've forgotten their authentication credentials aren't automatically accused of fraudulent behavior, he adds.

After learning how BioSig-ID worked, Tri-C reached out to the company, created a faculty committee that included IT, and conducted several demonstrations to understand the product and how it would report its findings to faculty members should a user be flagged by the system. Tri-C then pulled together resources and ran a one-semester test of BioSig-ID with two faculty members in the spring of 2014.

"We did one term where we created a sandbox in Blackboard for them to play around and understand how the product worked," Dull adds, explaining that faculty learned how to use BioSig-ID as a standard sign-in for classes, or as just an added authenticator for students to use prior to taking an online test. Tri-C also used that test period to see "would students see gesture-based authentication as an additional hurdle to get into class? Are they going to complain that it is too cumbersome?"

Tri-C found that the system wasn't a turn-off for students. It takes roughly five minutes to set up and can be used on computers, tablets, and mobile devices, making it easy for students to use the verification tool on any technology format.

Another factor that plays in Tri-C's favor is that many students are also taxpayers in the county. "So there's a much stronger connection between our community college and our students," Dull explains. "They really appreciated the college taking a step to do something to provide better resources for students—because if we have fraud, that's money we can't put towards education."

BioSig-ID will also ensure that Tri-C remains compliant with the new regulations that Dull was originally concerned with. One is within the reauthorized Higher Education Act, which requires institutions that offer distance education—like online classes—to have a process to establish that the student who registers in a class is the same student that participates in, completes, and receives credit for that class.

Tri-C has not expanded the use of BioSig-ID beyond the trials run in 2014, but it is in the process of securing the final approval from the administration to implement the solution campuswide for any secure interaction with the college online, Dull says. ■



FOR MORE INFORMATION:
Biometric Signature ID, www.biosig-id.com, 877/700-1611 ext. 53