An Acxiom White Paper

Methods to Verify the Identity of Distance Learning Students

ACXIOM®
WE MAKE INFORMATION INTELLIGENT™

To ensure integrity in online education, the distance learning industry is expanding strategies to verify the identity of distance learning students. The preferred approach now is not just to verify user IDs and passwords, but to also increase certainty that the individual getting credit for work actually did the work.

Online versus face-to-face

The widespread adoption of the Internet brought changes to nearly every aspect of our lives. Each industry has been forced by commercial, regulatory and competitive forces to adapt from a face-to-face dominated world to one that provides on-demand, 24/7 telephone, email, and Web delivery models for every component of a relationship. Different practices and rules evolved, and consumers in many industries now have different expectations for online versus face-to-face interactions.

Industry	Variations in Online versus Face-to-Face
Video and Book Retail and Rental	Product research and product referrals Public consumer reviews Real-time price comparison Inventory availability direct-to-consumer Trade-off of shipping costs versus drive time New online order and store pick-up policies New coupon redemption and return policies New privacy and security policies
Retail Banking	Different rates and fee structures Cost per transaction differences Decrease in personal face-to-face services New automatic bill paying service New regulations from the Electronic Funds Transfer Act of 1978 New privacy and security policies
Higher Education	Elimination of location barriers for finding relevant courses Increased access for part-time adult learners Flexible term and session start frequency Rise in for-hire adjunct instructors for online courses New virtual graduation ceremonies New regulations from the Higher Education Authorization Act of 2008 New privacy and security policies

There are natural and expected differences between online education and face-to-face education, just as there are with online bookstores, DVD rental websites and online banking sites. The privacy and security policies created in each industry should balance the needs for consumer convenience, privacy regulations, IT security technology and economics.

In higher education, one new privacy and security policy being debated in 2009 is how to verify the identity of online students. The U.S. Department of Education, regional accreditors, colleges, universities and trade associations are resolving how to implement a new federal policy requiring steps to verify the identity of online students. There has always been a natural question in distance education — how do you know who's doing the work for the credit? It's not like retail banking or video rental with a shipping address. Education's value comes from the course work and interactions during classes, ultimately expressed in a degree granted for fulfilling the requirements of a program.

Ethics and cheating in education

Educators, students and parents would agree that having someone else take an online final or ghost-write a paper for a student would cheat the student of an education. We recognize that a segment of people will cheat if stakes are high and there is little deterrent. Donald McCabe, of the Management faculty at Rutgers University, published a well-publicized paper in 2001 titled "Cheating in Academic Institutions: A Decade of Research," which indicates that cheating is "prevalent" and "widespread."[1] In late 2007 at one Florida institution, there were claims that 23 athletes cheated on Internet delivered assessments.[2] In the U.S. Army, its largest online testing program was compromised by thousands of students. The Army has since implemented comprehensive policies and technologies to increase integrity in the evaluation of 300,000 active and reserve soldiers.[3] Students and parents freely admit cheating is common in college and yet it's difficult for institutions to acknowledge unethical behavior, just as an online banking firm would hesitate to admit being a victim of fraud because of potential damage to its brand reputation.

Because of the fast growth and wide acceptance of distance education and concerns about potential financial aid fraud, the U.S. Congress has mandated improvements in the integrity of online higher education.

Higher education industry regulations

The higher education industry regulates itself via accreditation. "Accreditation is a process of external quality review used by higher education to scrutinize colleges, universities, and educational programs for quality assurance and quality improvement," according to the Council for Higher Education Accreditation.[4]

U.S. accreditors are now required to ensure that institutions with distance education programs have policies to verify the identity of distance learning students. Specifically, the Higher Education Act of 1965 (HEA) was renewed on August 14, 2008. In this bill, the Department of Education *"shall not require an accreditor to have separate standards, procedures or policies for evaluation of distance education. Accreditors must, however, require institutions that offer distance education to establish that a student registered for a distance education course is the same student who completes and receives credit for it,"* according to the American Council on Education Analysis of Higher Education Act Reauthorization.[5]

The Senate published a Joint Explanatory Statement of The Committee of Conference that further outlined that, although the current technology of user IDs and passwords are sufficient, *"As technology develops over time, the Committee anticipates that additional identification technologies will become more sophisticated, less expensive and more mainstream. The Conferees do not intend that institutions use or rely on any technology that interferes with the privacy of the student and expect that students' privacy will be protected with whichever method the institutions choose to utilize."*[6]

How the distance education industry regulates itself on this issue will be determined in 2009 in a process called Negotiated Rule Making. This is a third-party facilitated negotiation between the Department of Education and those who will be affected by new regulation, namely the accreditors and colleges and universities.[7]

Distance education requirements for identity

In 2005 Acxiom Corporation clients asked for technology solutions to ensure students who take an online course are who they say they are. Together with clients, trade associations and accreditor input, Acxiom researched the academic and IT requirements of possible solutions to this question. Academic deans, distance learning administrators and heads of distance education programs outlined key requirements to fit the needs of the diverse higher education market. Solutions needed to:

- Support, not prevent or disrupt, learning
- Be integrated in the learning process
- Be simple and flexible to deploy
- Be secure, non-invasive and not diminish privacy
- Be low-cost

In a 2006 session at one well-known university with more than 10,000 graduate and undergraduate online students, we at Acxiom reviewed the HEA language and the school's IT capabilities and online programs. We debated a practical implementation process with academic deans, the registrar and other university officials. The debate focused on academic integrity, the language in the HEA and the desired intent of the legislation and a practical application of identity verification in daily operations. We came to several conclusions that have been validated by other distance education providers through comprehensive solution evaluations and use in online programs.

The language from the HEA we reviewed is:

> *If such agency or association already has or seeks to include within its scope of recognition the evaluation of the quality of institutions or programs offering distance education, such agency or association shall, in addition to meeting the other requirements of this subpart, demonstrate to the Secretary that the agency or association requires that an institution that offers distance education programs to have processes by which it establishes that the student who registers in a distance education course or program is the same student who participates, completes academic work, and receives academic credit.*[8]

According to the legislation, there are four places for possible identity verification.

Specific Points for Authentication	Comments
"Registers in a distance education course or program"	Identity does not need to be verified at this point because registration alone enables students to enroll in courses and begin the learning process.
"Participates"	Participation in distance learning varies by course, program and institution. This ranges from chat, threaded discussions, assessments, email and term papers, among other activities. Learning is a collection of all the components and interactions of a course. Each independent student/instructor interaction may or may not have sufficient weight to be a candidate for verifying the student's identity.
"Completes academic work"	Work completion ranges from simple email to complex month-long projects. A good assessment process demonstrates mastery of course material. Of assessment types, some are more prone to impersonation and fraud than others. For practical purposes, randomly verifying identity just before an online assessment is the best time and place to improve integrity, as well as meet the standard in the HEA. As a result, courses with high-value online assessments are good candidates for identity.
"Receives academic credit"	Students are not involved in the granting of credit. The time when grades are posted or when a student reviews grades is not a valid time to verify student identity.

Authenticating (a user ID)

The definition of authentication exists in the world of information technology security. "Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done through the use of logon passwords. Knowledge of the password is assumed to guarantee that the user is authentic."[9] In a distance learning system, if a user ID and password are shared between users, they are not an effective mechanism for verifying a student's identity.

In some industries user ID and password are sufficient. In online banking, consumers would not share user IDs and passwords because they want to prevent others from using their bank account. In distance education, it's different. Students who want another person to take an exam on their behalf would willingly share their user ID and password to achieve a certain grade, even if it explicitly violates IT, academic and ethics policies.

Authenticating (a person)

There are three common methodologies to prove we are who we say we are:

- "Something we have" — a driver's license, access card or key
- "Something we are" — a biometric such as a fingerprint
- "Something we know" — a password or other common information about ourselves (such as a Social Security Number, mailing address, or our mother's maiden name)[10]

There are also systems that verify people's locations via callbacks, IP addresses or GPS tracking devices. These are known as "where we are" solutions.

Using two or more techniques is called two-factor authentication, and various industries have viable authentication solutions for specific applications. Banks now use shared secrets (password plus last four digits of SSN, or mother's maiden name). Online retailers use the CVC2 code on the back of a credit card as an extra precaution to prevent "CNP," or Card Not Present, fraud.

When applying these methodologies to distance education, we learn that each has significant drawbacks for use in distance education.

- "Something we have" is sharable. The digital token has a major drawback — hand it off and the student's quiz-taking partner assumes the registered user's identity. Devices require enrollment, tracking and a break/fix process, which increases costs and administrative requirements.
- "Something we are" requires devices to read the human body and a comprehensive enrollment process to capture identity prior to use. These systems also require end-user and administrator training. Costs tend to be higher with these solutions due to the required infrastructure.
- "Where we are" offers solutions for determining a user's location, but students move from home to work to library, making it impractical to predict when and where a student takes an online assessment.
- "Something we know" solutions offer low cost and high flexibility, provided they are embedded in the learning management system and do not leverage shared secrets that the student gave to the institution during enrollment or to their quiz-taking partner.

Over the past year, several approaches have been tested and are now generally available. These solutions should be used in addition to current academic integrity tools, such as plagiarism detection databases, encrypted test question banks, specialized Internet browsers to prevent browsing for answers, as well as comprehensive published policies for impersonation, cheating and ethical violations. Some distance courses are best suited for traditional face-to-face proctors, while others can leverage a Web proctor. Other online courses can rely on the less intrusive challenge question methodology to verify the student's identity.

Some IT leaders in higher education favor the use of challenge questions from an outside source, as they offer benefits over internal "shared secrets" (mother's maiden name, favorite color, etc.) between an institution and a student. First, IT systems in higher education are distributed and more open than in other industries. This has led to a large number of data breach incidents in higher education. Data about a student is often out of date, so relying on distributed, potentially latent data creates new exposure and risk of using this data in a new area. Second, strong online challenge question processes are patent protected, potentially requiring each institution to secure rights to leverage the technology. Third, the market for authentication solutions is rapidly evolving. Three years ago, using Social Security Number as a student ID was in favor. In three more years, the methods to protect people's data and the methods to beat these protections will be radically different than those utilized in 2009. If an institution's mission is to educate, many say an IT leadership team should not commit resources to building authentication technologies.

The following table outlines four primary available approaches at the start of 2009.

	Challenge Questions	Biometrics and Web Video Recording	Web Video Conference Proctor	Face-to-Face Proctored Exam
Methodology	Challenge questions based on third-party data.	Unique typing style or fingerprint plus targeted recording of student in exam via webcam.	Audio and video conference proctoring via webcam. Screen monitoring service with live, certified proctors.	Face to face with government or institution issued identification.
Mainstream Use	Widely used in financial services.	New, rarely used.	New, but used in family communications.	Commonly used.
Sophisticated	Yes. Based on large-scale databases of U.S. public records.	Yes. Uses newest web conference technology and biometrics or unique typing sequencing.	Yes. Uses newest Web conference technology.	No
Privacy	Student releases directory data to a third party. Institution never sees/receives data. Leverages publicly available data from prior address, phone and other available data. No FERPA violations. Covered by Gramm-Leach-Bliley Act and Driver's Privacy Protection Act.	Institution has access to videos of students taking assessments. Need policies for video review, use and release. Maintain database of student ID, directory information and student fingerprint or unique typing sequence.	Students participate in audio and video broadcast during exams. Proctor conducts exams from start to finish, with no intervention required from institution.	Student shows government-issued ID at approved facility.
Technical Pre-requisites	Integration to learning management software. Dial-up Internet connection. Secure access to third-party system.	Proprietary software, integration to learning or assessment software and broadband.	Commercially available webcam and broadband.	Varies by location. May require special software and PC. Each location requires review by academic staff.
Student Enrollment or Registration Process	None required. Supports walk-up students.	Capture fingerprint, typing samples or digital pictures. Device registration for student and student's PC. May require student signature on consent form.	Acquire webcam upon enrollment. Student schedules exam with proctor via scheduling system.	Usually none for on-campus facilities. May require pre-registration of exam time, location and proctor.

— continued on next page

	Challenge Questions	Biometrics and Web Video Recording	Web Video Conference Proctor	Face-to-Face Proctored Exam
Administration or Academic Staff Efforts	Determine when to pose identity questions. Determine ramifications of failure to authenticate. One-time distance learning staff involvement to set up process and program monitoring.	Set up course assessment in software, or integrate to learning software. Troubleshoot devices and user training, and monitor post-assessment video or audio. Manage device availability, inventory, assignment to students and break/fix process. Program monitoring to oversee usage.	Instruct students to schedule exams with proctor. One-time distance learning staff involvement to set up process and program monitoring.	Proctor must ensure student complies with proctored exam policies and procedures. (No calculator, no notes, etc.) Staff to verify proctor quality, proctor facilities, time, exam shipping, etc.
Additional Institution or Student Costs	None	Server software and database applications. Shipping costs for special device. May require specialized webcam or PC software.	Purchase of a standard, sound-equipped webcam.	Varies. Some institutions have no-cost testing facility sharing agreements, others charge for access. Some remote facilities charge $15 to $75 per assessment.
Investment (Assuming six courses per year and two assessments per course)	$2–4 per exam $8–18 per student per year	$25–45 per exam $150–270 per student per year	$15–20 per exam $90–120 per student per year	Varies from free to $75 per exam

Assessment strategies drive identity requirements

At institutions that use and implement the challenge question methodology, academic leaders reviewed assessment strategies in their online courses to help decide when and where to verify student identity. Program deans concluded courses with high-value online assessments and little instructor interaction are most likely candidates for comprehensive student identity verification. Advanced-level courses with face-to-face, threaded discussions, term papers or complex projects are less likely to have the same identity verification requirements. Just as assessments differ across community colleges, lower- and upper-level undergraduate and graduate programs, identity verification coverage should also be different. Some distance education institutions avoid online objective assessments in favor of subjective assessments, group projects, participation and other methods of assessing an individual's learning. With a new ability to verify the identity of an online test taker, instructional designers may now include objective assessments in their arsenal of assessment strategies where appropriate.

Conclusion

Other industries that have online and offline interactions have developed processes for ensuring integrity to achieve a specific objective, such as secure online banking or credit card transactions. The distance education industry is now reviewing the best methods to increase academic integrity by implementing identity verification for distance learning students to meet the demands of new legislation and diverse distance education programs. Institutions need to evaluate their online assessment policies and match the right level of identity verification to meet the new federal requirements to ensure the student who enrolls is also the student who does the work and gets the credit.

Michael Jortberg is the Higher Education Market Leader at Acxiom Corporation, which integrates data, services and technology to create and deliver customer- and information-management programs and systems for clients. He can be reached at Michael.Jortberg@Acxiom.com.

Notes

[1] Cheating in Academic Institutions: A Decade of Research
http://www.swarthmore.edu/NatSci/cpurrin1/plagiarism/docs/McCabe_et_al.pdf

[2] Nearly 2 dozen Florida State Athletes Accused of Cheating
http://www.usatoday.com/sports/college/2007-09-26-floridast-cheating_N.htm

[3] Catching the Cheaters
http://www.armytimes.com/careers/pme/mcitesting9.4/

[4] The Fundamentals Of Accreditation
http://www.chea.org/pdf/fund_accred_20ques_02.pdf

[5] ACE Analysis of Higher Education Act Reauthorization
www.acenet.edu/e-newsletters/p2p/ACE_HEA_analysis_818.pdf

[6] Joint Explanatory Statement Of The Committee Of Conference
http://help.senate.gov/Hearings/2008_07_29_E/Statement_of_Managers.pdf

[7] The Negotiated Rulemaking Process for Title IV Regulations – Frequently Asked Questions
http://www.ed.gov/policy/highered/reg/hearulemaking/hea08/neg-reg-faq.html

[8] Text of H.R. 4137: Higher Education Opportunity Act
http://www.govtrack.us/congress/billtext.xpd?bill=h110-4137

[9] SearchSecurity.Com Definition of Authentication
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html

[10] Symantec Security Forum
https://forums.symantec.com/t5/Online-Fraud/Phishing-and-Two-Factor-Authentication-Revisited/ba-p/306184#A50

See how Acxiom can work for you.
For more information, visit our website at
www.acxiom.com/education or call:

1.888.3ACXIOM

AC-0031-09 ELEC 1/09