Online Learner Authentication: Verifying the Identity of Online Users

Jeffrey L. Bailie
National American University
Rapid City, SD 57701 USA
jbailie@national.edu

Michael A. Jortberg
Acxiom® Corporation
Downers Grove, IL 60515 USA
michael.jortberg@acxiom.com

Abstract

This paper addresses how one university has partnered with a corporation to work on the verification of online student identity and describes ongoing efforts to best verify online student identity. Through this collaboration, the university seeks to enhance the credibility of its online evaluation process by employing data forensic techniques commonly used by today's financial services industry. Detail is presented on how user authentication strategies are being applied to verify remote learner identity during formal online performance appraisals. Additional details on how the existing strategies will be enhanced toward multi-faceted user authentication are discussed.

Keywords: Online Learning Student Authentication/ Online Education User Identity

Introduction

Perhaps more than ever before, today's adaptation of distance education offers a ubiquitous academic substitute to the traditional classroom experience for students who desire a learning opportunity that is more convenient for their individual lifestyle. Many of the advancements that have allowed for a more convenient system of delivery have materialized as technology continues to influence the landscape of distance education (Cole, 2000). Increasingly, online course offerings are viewed as somewhat of a necessity for universities as they strive to meet the changing interests of a savvy constituent base that demands a wide range of options in their scholastic pursuits (Wilson & Moore, 2004). Barriers of time and place that once created impediments to enrollment are now overcome through the relative flexibility found in Web-based delivery. Yet while technological advancements of the past decade have leveraged the "any time/any place" advantage often associated with online learning, similar progress to create a regulated environment for controlled activity has been somewhat of a challenge (Heberling, 2002).

Historically, the assessment of student learning at a distance has not been without controversy. After all, how the identity of an individual completing such coursework is validated has been the basis of scorn by those critical of distance education for decades. More recently, verbiage in Public Law 110–315 (United States Higher Education Opportunity Act, 2008) directs accreditation agencies to require an institution to have processes to establish that the student who registers in a distance education course or program is the same student who participates in and completes the program and receives the academic credit. As a result, institutions of higher learning have found it necessary to contemplate various solutions surrounding their approach to assessing the performance of remote learners.

In response to the federal mandate, The Higher Learning Commission (HLC) drafted a new policy on verifying identity of students in distance and correspondence education. The recently adopted HLC policy requires that:

> Institutions offering distance education or correspondence education, as specified in the federal definitions reproduced herein solely for reference, shall have processes through which the institution establishes that the student who registers in the distance education or correspondence education courses or programs is the same student who participates in and completes and receives the academic credit.

The Joint Conference Committee of Congress and the U.S. Department of Education have confirmed that initially institutions may use simple efforts already in place at most institutions to verify identity. Such efforts may include the use of IDs and passwords. The HLC policy reflects this current understanding; however, as better processes for verifying the identity of students come into existence over time and as final regulations develop, this policy may need to be updated (Higher Learning Commission, 2009).

Fraud in Academia

Unlike an online bank with deposit transfer capabilities, a university with an online program is not a target for a student to break in and steal an education. However, this does not mean there is not concern about academic integrity. In other industry sectors, fraud is managed by the risk mitigation function. In academia, the academic integrity policies are managed by faculty and academic leaders. Because of such differences, business requirements for technology solutions are of different designs that meet the unique service needs of the industry. Instances of fraud commonly include three recognized conditions, known as the "Fraud Triangle." The three conditions that form the triangle include an opportunity, an incentive or reward, and a rationalization. When all three conditions are present, corresponding fraud may appear (Wells, 1997). I In a study of 476 business students, researchers found that when each element of the fraud triangle is reduced, the result is a significant determinant in student cheating (Becker, Connolly, Lentz, & Morrison, 2006). The results of another study suggest that 73.6% of the students in the sample held the perception that it is easier to cheat in an online versus traditional course (King, Guyette, & Piotrowski, 2009).

User Authentication

Authentication is a common term expressed in the information technology security industry. The term authentication has been defined as 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), the process of authentication is commonly completed through the use of logon user identification and passwords, and the knowledge of the password is assumed to guarantee that the user is authentic (Ramzan, 2007). Needless to say, if a password is shared between users, its use cannot be viewed as an effective mechanism for verifying user identity. User IDs and passwords were called out for having many well-known vulnerabilities, and security analysts suggested that organizations should plan for stronger authentication for system administrators and other privileged users, by year-end 2007, and for primary network login for all users by 2009 (Allen, 2007).

In some industries, user ID and password may be sufficient for authentication because they are inherently secured by the user. Some industries, such as banking and online retail, invest in a second layer of protection to ensure risks are mitigated. In online banking, for example, consumers refrain from divulging their assigned user ID and password to prevent others from accessing their bank account. Resetting a password usually triggers a second layer of identity verification. In online education, dishonest students willingly reveal their user ID and password to others for the purpose of cheating, even if it explicitly violates academic policies on student conduct.

In response to growing concerns over academic honesty in the online environment, Excelsior College of Albany, New York has included a specific statement about identity fraud in their academic honesty policy. The policy states that all forms of academic dishonesty are considered serious violations of the ethical standards of Excelsior College, but one that is considered particularly egregious is identity fraud. Any student who has another person impersonate or in any other way commit identity fraud in any course, exam or other academic exercise will be dismissed from the college. (Excelsior College, 2009)

Over the past few years, varied approaches to user authentication in the online learning environment have been tested and are now being incorporated into online learning ventures. In many cases, such alternatives have served as substitutions to the conventional means of on-site, face-to-face examination sessions including:

- Even with these available alternatives, the pressure continues to mount to find a trustworthy yet cost-effective Use of proctored assessments administered through sanctioned testing centers;
- Use of advanced technology intended to validate an individual's biometrics including fingerprint readers, signature, facial, or voice recognition programs;
- Synchronous monitoring including Web video recording or monitoring, telephone call-back, IP monitoring, or software that detects discrepancies in response patterns such as how an individual types;
- Increased emphasis on student portfolios, papers, projects and quizzes in exchange for high "point weighted" midterm and final examinations;
- Avoidance of an objective assessment and controlled testing settings by using various methods to assess learning

Even with these available alternatives, the pressure continues to mount to find a trustworthy yet cost-effective protocol to securely evaluate students engaged in online learning. Also, given the wide variety of distance education venues and the varying assessment methodologies now available, one strategy will not fit all situations. In addition, proving identity in every situation that a student performs is not realistic, practical or cost effective. According to a 2005 report issued by the Illinois Community Colleges Online, assessment in online courses falls into 10 broad categories as denoted in Table 1.

Table 1. Types of Assessment on Online Learning

Responses	Frequency	Percent
Homework assignments	655	20%
Online tests and/or quizzes	606	19%
Bulletin-board postings	547	17%
Projects/papers	494	15%
Participation in chat room	313	10%
Proctored tests and/or quizzes	234	7%
Team projects	149	5%
Reflective journal	92	3%
Student portfolio	79	2%
Other	31	1%
Total	3,200	

Acxiom Corporation conducted interviews between 2006 and 2008 with distance learning program leaders, IT technical professionals and academic leaders and found that the requirements for identity verification became clearer based on the nature of distance learning programs. Important considerations included cost, flexibility and simplicity. As a result of these interviews, and the new nature of identity verification in distance learning, the initial focus was on a technology solution directed toward the online assessment process. Participants involved in the interview process outlined the need for basic functions that could evolve as the distance learning industry addressed the new need for identity solutions in online courses. A critical requirement identified was the expressed need to increase student satisfaction and yet not interfere with learning and a student's privacy (Jortberg, 2009).

As of May 2009, several methodologies are available on the market to address identity in distance education in addition to user id and password. The following outlines the types of solutions and criteria about each. They are:

- Biometrics and Web Video Recording: Unique typing style, signature, voice or fingerprint plus targeted recording of student in exam via webcam
- Challenge Questions: Challenge questions based on third-party data
- Face-to-Face Proctored Exam: Face to face with government or institution issued identification
- Web Video Conference Proctor: Audio and video conference proctoring via webcam. Screen monitoring service with live, certified proctors.

Privacy: What is the privacy impact of each methodology?

- Biometrics and Web Video Recording: These solutions require capture and storage of unique identifying characteristics of the student.
- Challenge Questions: Challenge questions based on third-party data. Based on public and private data, these solutions pose questions to a student just before an assessment. This data is not covered by FERPA but the use is governed by Gramm-Leach-Bliley Act and Driver's Privacy Protection Act.
- Face-to-Face Proctored Exam: Proctored exams typically require a photo id and have little impact on privacy.
- Web Video Conference Proctor: Because the exam session is not recorded, there are no significant privacy concerns.

Technical Pre-Requisites: What are the pre-use technology requirements of each methodology?

- Biometrics and Web Video Recording: Proprietary software, integration to learning or assessment software and broadband internet connection.
- Challenge Questions: Requires integration to learning management software and minimum dial-up Internet connection as well as secure server access to third-party challenge question database.
- Face-to-Face Proctored Exam: Varies by location. May require special software and PC. Each location requires review by academic staff to ensure proctor quality and compliance to institution test center standards. Students adhere to proctor center test hours.
- Web Video Conference Proctor: Commercially available webcam and broadband internet. Student Enrollment or Registration Process: What are the steps required before use in an online assessment?
- Biometrics and Web Video Recording: Capture fingerprint, typing samples, voice, signature or digital pictures. Device registration for student and student's PC. May require student signature on consent form.
- Challenge Questions: None required. Supports walk-up students.
- Face-to-Face Proctored Exam: Requires pre-registration student, exam, exam date and time, location and proctor. (see Figure 1)
- Web Video Conference Proctor: Acquire webcam upon enrollment. Student schedules exam with proctor via scheduling system.

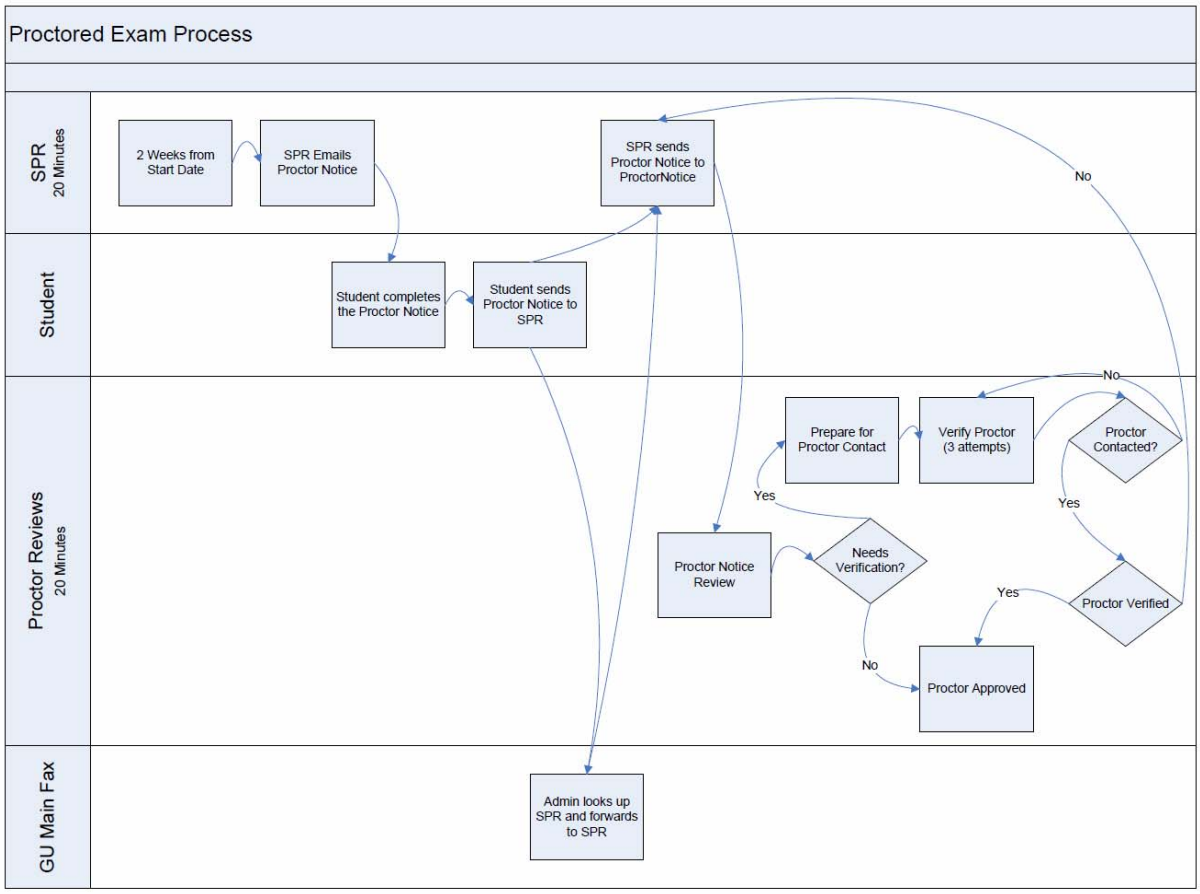
Administration or Academic Staff Efforts: What are the instructor and administrative functions required prior to use in an online assessment?

- Biometrics and Web Video Recording: Set up course assessment in software, or integrate to learning software. Troubleshoot devices and faculty and student training, and monitor post-assessment video or audio. Manage device availability, inventory, assignment to students and break/fix process. Program monitoring to oversee usage.
- Challenge Questions: 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.
- Face-to-Face Proctored Exam: 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. (see Figure 1)
- Web Video Conference Proctor: Instruct students to schedule exams with proctor. One-time distance learning staff involvement to set up process and program monitoring.

Additional Institution or Student Costs: What are the total operational cost items required to support the methodology?

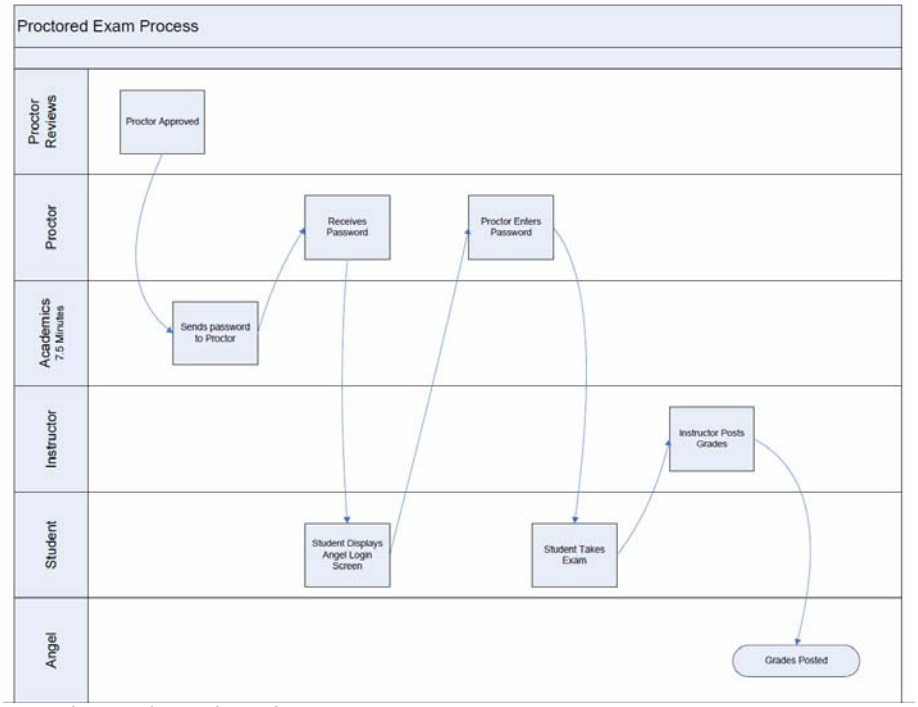
- Biometrics and Web Video Recording: Device, server software and database applications. Shipping costs for special device. May require specialized webcam or PC software.
- Challenge Questions: Subscription to challenge question database.
- Face-to-Face Proctored Exam: Varies. Some institutions have no-cost testing facility sharing agreements, others charge for access. Some remote facilities charge $15 to $75 per assessment. Travel expenses and time. Administrative staff salary and time.
- Web Video Conference Proctor: Purchase of a standard, sound-equipped webcam. Subscription to web proctor provider.

Figures 1a and 1b depict the institutional and student process for proctored examinations as required by Grantham University (Grantham University Institutional Research). The task complexity depicted in this process might be considered as the rationale for why complete reliance on face to face proctoring can be cumbersome to manage, as well as being inconsistent with "any time – any place" attraction of distance education. In the case below, the proctor verification process is more complex than some of the emerging student verification processes.



SPR = Student Progress Representative
GU = Grantham University

Figure 1a. Grantham University's Proctor Verification Process



Angel = Angel Learning software

Figure 1b. Grantham University's Proctored Online Exam Process

A Piloted Solution

During 2008 and 2009, in collaboration with Acxiom Corporation and Blackboard Inc., National American University (NAU) has successfully tested a solution intended to be an additional step in the identity verification of remote learners enrolled in the university's online courses. Through this approach, as depicted in Figure 2, select student directory information (released by students) is recognized by a third-party authentication service based on a variety of public and private sources outside of the university (managed by Acxiom), and routed through the learner management system (Blackboard Inc.) via a Web interface.

With the resulting information, users are presented with challenge questions before they can gain access (or continue) to a secured assessment. Used in addition to other academic integrity tools such as plagiarism detection databases, encrypted test question banks, and published policies, this feature is viewed by NAU as an opportunity to further ensure integrity in their online evaluations. Consistent with the challenge question approach used extensively in the financial services, online retail and insurance industries, the project required each student to supply data representative of the "what we have" (in the form of user ID and password) along with "what we know" (responses to third-party challenge questions) protocol to verify online student users. The scenario is as follows:

1. Courses that will include a challenge question authentication are selected. Students enrolled in the course are informed of the approach and offered an opportunity to opt out. The alternative to participation is the conventional proctored arrangement.

2. Participants enter the learner management system (Blackboard CE 8) in a conventional fashion, by use of an assigned user ID and password issued by the university. Using this detail, students access their assigned course.

3. When entering a "trigger event," such as an exam, a series of challenge questions are posed for further authentication. Challenge questions may be posed before the exam, as determined by the university. Unanswered or incorrectly answered challenge questions restrict progress to

the authorization feature. NAU determines tolerance on challenge questions including timing, number and frequency. In addition, NAU decides how to resolve situations when students do not pass the series of challenges.

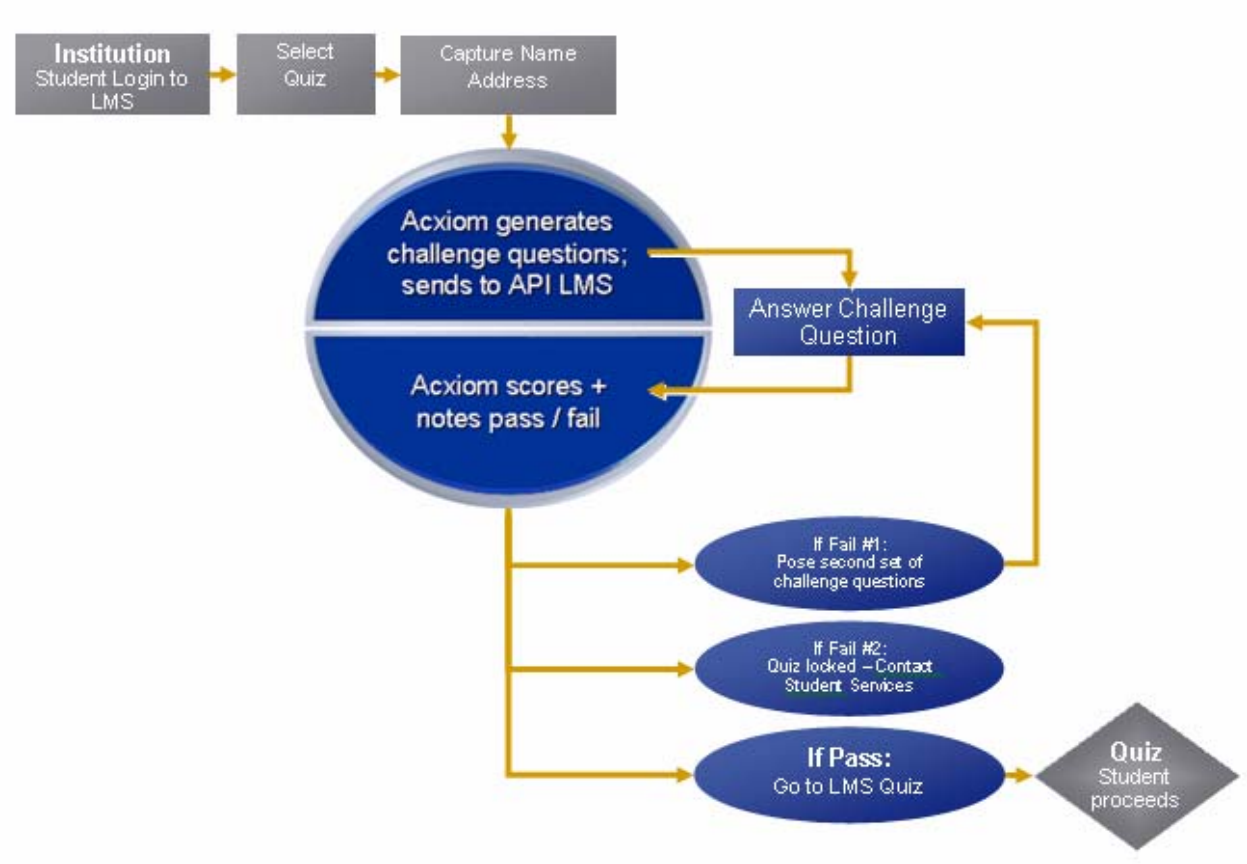


Figure 2. Acxiom – Blackboard – NAU Approach

The application presents challenge questions based on public and private data compiled and managed by a third party for use in risk mitigation solutions. The available data can be utilized to create from 150 to 300 challenge questions per individual. As a result, each student receives a different set of challenge questions during each assessment. Random coverage of various assessments ensures students do not detect a pattern in the challenge question timing and mitigates an individual's ability to have a partner assist with every assessment in their academic career.

During three tests of the solution (February 2008, October 2008, and February 2009), online students from NAU and other participating institutions were presented with challenge questions. Data representative of one student population set is listed in Table 2. Ongoing use, reporting and policies are being developed to best address how academic leaders will leverage this information in their quest for academic integrity.

During spring and summer 2009, additional institutions will begin posing challenge questions through Blackboard, Moodle, Angel and other learning software systems. The aggregate results of these early users of this new technology will be shared in subsequent papers. These systems support many types of online assessments, including the most common as captioned in Table 3.

Table 2. Results of 2008-09 Pilot Tests

Identity Verifications	Passed	Passed %	Failed	Failed %	Incomplete	Incomplete %
16	15	94%	0	0%	1	6%
26	23	88%	2	8%	1	4%
22	21	95%	0	0%	1	5%
30	27	90%	0	0%	3	10%
27	24	89%	0	0%	3	11%
29	28	97%	0	0%	1	3%
33	31	94%	1	3%	1	3%
Total: 183	Total: 169	Average: 92%	Total: 3	Average: 2%	Total: 11	Average 6%

Note. Identity Verifications shows the number of requested exams. Pass shows the number of students who confirmed their identity. Failed shows the number of students who did not answer the challenge questions or subsequent follow-up challenge questions accurately. Incomplete means the student was presented with the challenge questions but did not complete the identity verification process. These results are shared with faculty and staff to either address students or modify the challenge question process to better fit the population and increase effectiveness of the solution.

Table 3. *Common Types of Online Assessment Types*

Algorithmic/Numerical	Embedded Answers	Opinion Scale / Likert
Calculated Formula	Fill in the Blank	Ordering
Description	Jumbled Sentence	Random Short Answer Matching
Either/Or	Multiple Choice	Short Answer

Student Feedback

In addition to the benefit student authentication projects lend to an institution, the satisfaction of the online student consumer must also be measured. Early survey results from student use have been positive. The results of a 2008 survey of student regarding their satisfaction with the authentication solution are offered in Tables 4 and 5.

In subsequent surveys, one student stated “I think this is a great idea and would make it so much easier to take tests if a proctor was not required.” In spring and summer 2009, students, academic leaders and distance education professionals who have used the system will be surveyed and results will be published. This group of 10 institutions with distance education programs represents four- and two-year public and private for-profit and non-profit institutions.

Table 4. Results of 2008 Student Satisfaction Survey

Question	Yes	No
Have you been through a verification process similar to this in the past?	74% / 19	26% / 5
Were you able to answer these questions without any reference materials?	100% / 18	0% / 0
Would you prefer to use this verification process instead of a proctor in the future?	94% / 17	6% / 1
Have you ever had to use a proctor for an NAU course?	72% / 13	28%/ 5

Table 5. Results of 2008 Student Satisfaction Survey

Question	Hard	Moderate	Easy	Very easy
How difficult did you find answering the previous questions?	0% / 0	17% / 3	22% / 4	61% / 11

Costs and Savings

As with any legislation, the Higher Education Opportunity Act led to a scramble by market participants to fulfill the requirements. In 2009, the U.S. Department of Education is holding the Negotiated Rulemaking process to better define how to implement all the changes. Included in this rulemaking process is the distance education identity requirement. While many market participants assume new regulations force unfunded changes, this project has demonstrated that legislation can force new solutions that create effective uses of new technology with a positive impact, such as reduced costs, increased quality and increased student satisfaction.

Institutions that rely on proctored exams feel a shift to online identity verification from face to face will reduce administrative costs at institutions, increase student satisfaction and save time and energy by reducing travel or time off work to test facilities. Institution leaders report that the process of identity verification increases quality and integrity of online programs. IT security professionals in higher education see many uses of online identity verification beyond distance learning to include a stronger password reset process, enhanced security in student cash and debit card activation and initial user ID provisioning. Each of these applications of identity verification also can reduce operational costs and increase quality in the respective departments.

Multifaceted Expansion of Online Authentication

As the pilot project successfully emerged, dialog focused on the potential for additional benefit that could be captured from the solution's use. It was determined that, beyond online examinations, a variety of other interface episodes common to online learning could include the authentication protocol. In fact, user authentication could realistically be required anytime a new Web page is opened within the online learning environment. Conceptually, an institution could require a user to complete the authentication steps in conjunction with activities such as logging in to the course, posting to a discussion, joining a chat session, or uploading a paper.

The true benefit gained by an institution's agility in the placement of the authentication event to coincide with graded exercises aside from examinations warrants further study. NAU is currently exploring additional authentication placements within select activities within the Blackboard LMS, assuming that the placement of the authentication protocol in exercises beyond examinations may very well inhibit a potential fraudster's capacity for advanced planning.

Conclusion

As illustrated in this paper, projects to further authenticate the identity of online students have been successfully piloted. While certainly not a panacea, academic institutions involved in end user authentication projects are hopeful that the success of these projects will increasingly contribute to the credibility of an institution's online delivery options by adding yet another step toward identity verification of online students situated throughout the world. A list of Frequently Asked Questions (FAQ's) common to this project is included as an appendix to this paper. The NAU - Acxiom project is viewed as an example of how the interests of higher learning and corporate entities have successfully anticipated, and collaborated to address, the challenges encountered as technology and market conditions change and advance.

References

Allan, A. (2007). *The Twilight of the Passwords: A Timetable for Migrating to Stronger Authentication*, Gartner Group. Retrieved March 10, 2009, from http://blog.gartner.com/blog/mediablog.php?itemid=2017

Becker, D., Connolly, J., Lentz, P., & Morrison, J. (2006). Using the business fraud triangle to predict academic dishonesty among business students. *Academy of Educational Leadership Journal, 10*(1), 37-54.

Bruhn, M., Gettes, M. & West, A. (2003). Identity and access management and securityin higher education, *EDUCAUSE Quarterly, 26*(4),12-16.

Cole, R. A. (2000). *Issues in Web-based pedagogy: A critical primer.* Westport, CT:Greenwood Press.

Excelsior College (2009). Academic Honesty Policy. Retrieved April 26, 2009 from https://www.excelsior.edu/Excelsior_College/POLICIES/ACADEMIC_HONESTY_POLICY

Heberling, M. (2002). Maintaining academic integrity in on-line education. *Online Journal of Distance Learning Administration, 5*(2). Retrieved March 6, 2009, from http://www.westga.edu/%7Edistance/ojdla/spring51/spring51.html.

Higher Education Opportunity Act (2008). Retrieved March 1, 2009, fromhttp://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ315.110.

Higher Learning Commission (2009). *Summary of Policies Related to the Higher Education Opportunity Act.* Retrieved March 11, 2009 from http://www.ncahlc.org/download/Policies%20Adopted%20Final%202-2009.pdf.

Holohan, R., Fischbach, R., Fisher, R., Campbell, T., & Rohr, T. (2005). *ILCCO Research Report 2005: Quality, Retention and Expansion of Online Courses and Programs in Illinois Community Colleges.* Retrieved March 9, 2009 from Illinois Community Colleges Online Web site: http://www.ilcco.net/ILCCO/resources%5CILCCO%20Final%20Report.pdf.

Jortberg, M.A. (2009) Methods to verify the identity of distance learning students. *Acxiom White Paper.* Retrieved March 1, 2009, from http://www.acxiom.com/199626/AC-0031-09_DistanceLearningStudentsWP.pdf.

King, C.G., Guyette, R.W., & Piotrowski, C. (2009). Online exams and cheating: An empirical analysis of business students' views. *The Journal of Educators Online, 6*(1). Retrieved March 5, 2009, from http://www.thejeo.com/Archives/Volume6Number1/Kingetalpaper.pdf.

Nagy, A. (2005). The Impact of E-Learning, in: Bruck, P.A., Buchholz, A., Karssen, Z., & Zerfass, A. (Eds). *E-content: technologies and perspectives for the European market*. Berlin: Springer-Verlag.

Ramzan, R. (2007, May 17). Phishing and Two-Factor Authentication Revisited. Message posted to https://forums2.symantec.com/t5/Online-Fraud/Phishing-and-Two-Factor-Authentication-Revisited/ba-p/306184#A50

Search security.com definitions. (n.d.). Retrieved March 11, 2009, from http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci211621,00.html.

Wells, J.T. (1997) *Occupational Fraud and Abuse.* Obsidian Publishing Co: Austin, TX.

Wilson, E. & Moore, G. (2004). Factors related to the intent of professionals in agricultural and extension education to enroll in an on-line master's degree program. *Journal of Agricultural Education, 45*(4), 96-105.

Appendix: Frequently Asked Questions Relative to the Program

Why verify identity?

By verifying identity, we send a message that we are concerned that students receive the deserved credit for the work they are performing. We also demonstrate a proactive interest in compliance with any new requirements requiring a process to verify the identity of the student as being the same as the individual who registered for the course.

Why on-line and not in-person?

Because of vast expansion of enrollments in online courses, it became increasingly impractical to require students to report to a physical location for scheduled in-person identity verification. Third party in-person verification of today's contemporary and distributed learner population are logistically difficult, not as secure as desired, and costly.

How do you verify the identity of on-line learners?

We pose questions that require the student to answer questions about their demographics such as where they lived in the past or what type of car they have owned. These questions are data generated because they are from the past transactions and the data is not usually found in an individual's wallet. The questions are derived from public data sources and managed by a 3rd party, independent of our institution.

How do challenge questions work?

We posed challenge questions at select intervals prior to a testing session, offering students a predetermined response time to answer the questions.

What prevents a student from having someone else help them answer the questions?

Our approach is intended to be a barrier to fraudulent activity. While it is clearly not 100% failsafe, it is certainly consistent with practices of today's financial institutions who offer online services. We view this barrier as a sincere beginning to a program that will continue to advance. It is, if nothing else, a notable starting point that meets our current budget and policy requirements.

Why use an external data source to verify an individual's identity?

The volume of data in the US consumer market is larger than any individual academic institution can single-handedly manage. The challenge questions are much more than the typical "what is your mother's maiden name." Because the collection of identifying data is external to the school and not self directed challenge questions that the student gave to the school, the student can not predict the questions posed. This further increases the integrity of the application.

Manuscript received 17 Mar 2009; revision received 14 May 2009.