e-mentor
No 1 (38) / 2011
www.e-mentor.edu.pl/eng

Investigating and Implementing Online Student Identity Verification

Anthony A. Piña, Larry Bohn, Jeff Lyons

A technology-based system using personal questions to verify the identity of online students was implemented and field tested by a U.S. University. The field test included 112 students, 85 of whom completed a questionnaire about their experiences with the system. Data gathered from students, instructors and the system administrator indicated that the system was an effective and preferable way to verify the identity of online students.

One of the most persistent issues facing educational institutions that offer online programs is whether a given online student is actually the one who registered for the online course[1]. In light of recent cases of financial aid fraud[2], threats from diploma mills[3] and anti-distance learning sentiments from legislators[4] and faculty[5], online student identity verification has been brought to the forefront of the dialogue on distance learning.

NEW REGULATIONS

The renewal of the U.S. Higher Education Opportunity Act introduced new requirements for accrediting agencies[6]. One of these requirements is that accrediting agencies must verify that

---

[1] R. Epper, M. Anderson, L. McNabb, *Are your online students really the ones registered for the course? Student authentication requirements for distance education providers*, Western Cooperative for Educational Telecommunications, Boulder, 2008.
[2] N. Collins, *Woman sentenced to almost five years in federal prison for student loan fraud*, United States Attorney's Office, District of Nevada, Las Vegas 2006; W. Hornbuckle, *Ringleader of $500,000 financial aid fraud scheme sentenced to prison*, United States Attorney's Office, District of Arizona, Phoenix 2010.
[3] A. A. Piña, *How online diploma mills hurt e-learning*, „e-Mentor" 2009, No. 5 (32); A. A. Piña, B. R.Harris, *On verifying online student identity,* Annual convention of the Association for Educational Communications & Technology, Anaheim, October 2010.
[4] A. L. Foster, *A congressman questions the quality and rigor of online education*, „Chronicle of Higher Education" 2006, No. 52 (30).
[5] D. Shieh, *Professors regard online instructor as less effective than classroom learning*, „Chronicle of Higher Education", No. *55*, http://chronicle.com/article/Professors-Regard-Online/1519, [02.02.2011].
[6] V. Sampson, *Dear colleague: The higher education opportunity act,* Washington DC: Office of Postsecondary Education, U.S. Department of Education, 2008.

institutions with distance learning programs, "have processes through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the program and receives the academic credit"[7].

The six regional agencies that accredit higher education institutions in the United States have adopted language in their institutional policies and guidelines to reflect the new regulations. The following excerpt from the Commission on Colleges of the Southern Association of Colleges and Schools (SACS) is representative: "At the time of review by the Commission, the institution must demonstrate that the student who registers in a distance or correspondence education course or program is the same student who participates in and completes the course or program and receives the credit by verifying the identity of a student who participates in class or coursework by using, at the option of the institution, methods such as (1) a secure login and pass code, (2) proctored examinations, and (3) new or other technologies and practices that are effective in verifying student identification"[8].

Colleges and Universities that use learning management systems featuring secure logins and pass codes (e.g. Blackboard, Angel, Desire2Learn, Moodle, Sakai, etc.) are considered to be meeting the "letter" of this law, as interpreted currently by the U.S. Department of Education[9]. However, as a result of the publicity and excitement surrounding the new identity verification requirements, and in anticipation of more stringent interpretations of the law, vendors have responded with a number of solutions that vary widely in sophistication, complexity and price[10].

---

[7] Higher Education Opportunity Act (Public Law 110-315), 2008, http://ed.gov/policy/highered/leg/hea08/index.html, [02.02.2011].
[8] Commission on Colleges, *Distance and correspondence education policy statement*, Southern Association of Colleges and Schools, Decatur 2010, p.1.
[9] Commission on Colleges, *Distance education and the principles of accreditation: Documenting compliance guidelines*, Southern Association of Colleges and Schools, Decatur 2009.
[10] M. A. Jortberg, *An Acxiom white paper: Methods to verify the identity of distance learning students*, Acxiom Corporation, Little Rock 2009.

MULTIPLE SOLUTIONS

Jortberg[11] provided a useful and comprehensive matrix of the four most common methods to verify online student identity: in-person proctored examinations, audio/video conferencing using a webcam and live proctors, biometric/hardware scanning using fingerprint, eye, typing pattern or digital photograph recognition, and challenge questions based on third party data. For each of these methods, Jortberg described the methodology, applications, student enrollment process, administration/staff roles, cost of implementation, additional institution or student costs and limitations for each of the four methods[12].

TESTING THE OPTIONS

During a two year period, members of Sullivan University Global e-Learning conducted demonstrations and field tests of several different identity verification solutions, including those identified by Jortberg[13]. The hardware-based camera and scanner solutions required students to obtain, install and configure hardware and proprietary software and restricted student to using only those computers with the hardware and software installed. In a number of cases, the field tests of these products suffered from difficult configurations, hardware or software incompatibilities, poor connectivity or poor quality images. The costs for obtaining the hardware, shipping it to hundreds or thousands of students dispersed around the globe, and expecting students to configure the hardware and software correctly, made these solutions costly and unfeasible[14]. Concerns over the possibility of invasion of student privacy and potential liability were raised by some who felt uncomfortable with the idea of the University having the ability to watch (and possibly record) students in their homes and elsewhere.

The latest field test was performed on a system which utilizes system-generated personal challenge questions, based on publicly available data. The remainder of this paper will describe the implementation and evaluation of this solution with a group of undergraduate students enrolled in fully online courses.

---

[11] Ibidem.
[12] Ibidem.
[13] C. L. Scheidenhelm, A. A. Piña, J. Corliss, *Authentication of online students: Current practices*, The annual Supporting Learning and Technology in Education (SLATE) Conference, Chicago, October 2009.
[14] A. A. Piña, B. R.Harris, *On verifying online student identity,* Annual convention of the Association for Educational Communications & Technology, Anaheim, October 2010.

METHOD

Participants

The sample for this study included 112 undergraduate students enrolled in fully online sections of human resource leadership and medical coding courses.

Identity Verification Solution

The identity verification solution used for this study was Acxiom Identify-X. Acxiom is a billion-dollar corporation specializing in security, background checking and identity verification for banks, large financial corporations and other institutions. The Acxiom solution draws from an extensive public records database to create an historical profile and generate a series of personalized questions unique to each user in the system[15]. When students attempt to access an item in an online course that has been set up to use Acxiom, they are asked to enter their name, address and telephone number, which is authenticated in Acxiom's database and questions unique to the user are generated. By answering the questions correctly, the student's identity is verified. The identity verification can be applied to any content item in the LMS that can be hidden and displayed, but is most commonly utilized for quizzes, tests and other assessment items[16].

Integration with the LMS

Acxiom worked closely with ANGEL Learning, Inc. (now part of Blackboard, Inc.), to provide a seamless integration with the ANGEL Learning Management System. Integration is also available for a number of other systems, including Moodle and Blackboard's various products. The integration with ANGEL required minimal time and effort from the University's LMS Administrator—mainly involving pre-production testing of the system. The technical set-up for the LMS Administrator involved: 1) running a pre-packaged SQL server script, provided by

---

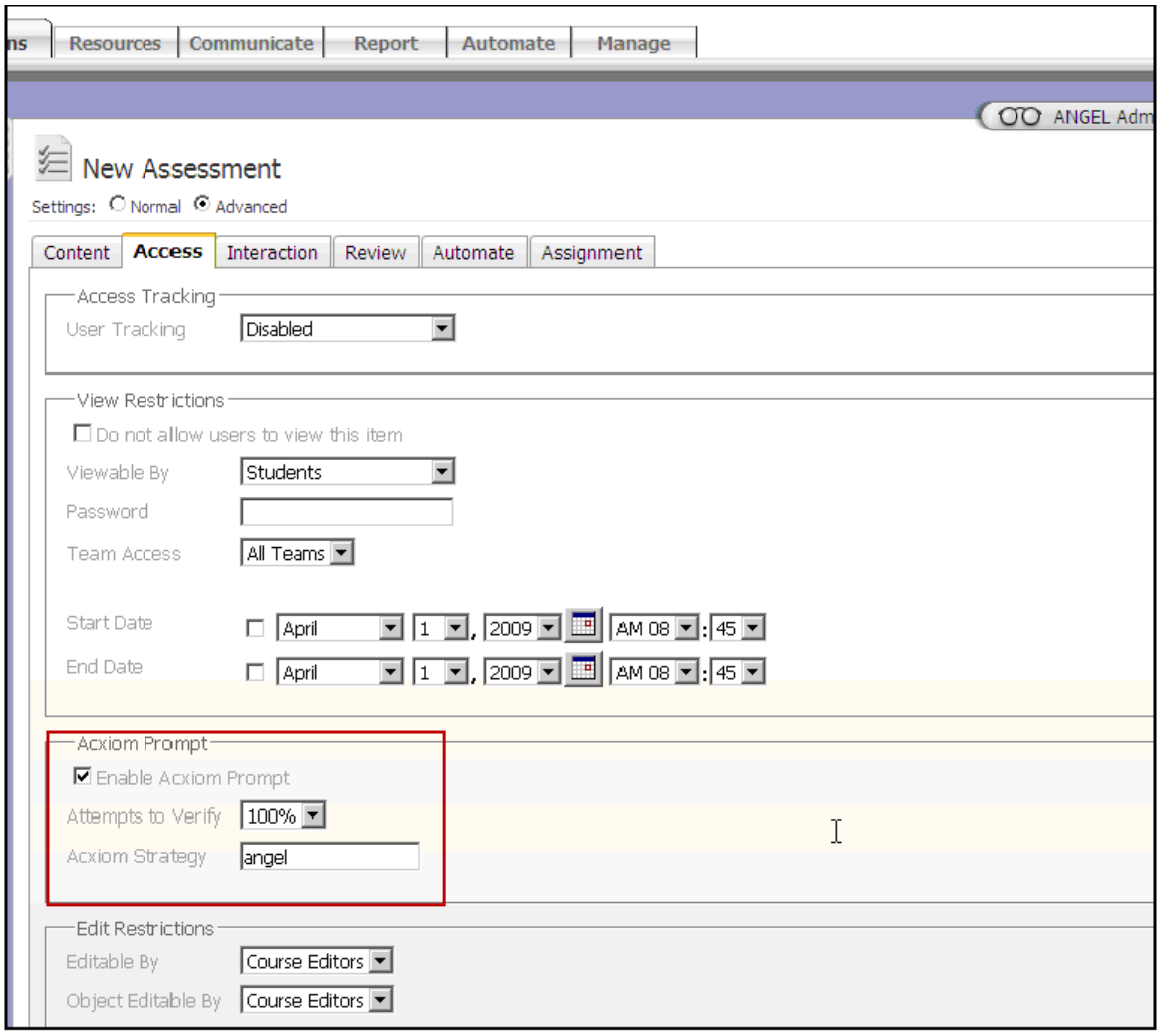
[15] M. A. Jortberg, op.cit.
[16] J. L. Ballie, M. A. Jortberg, *Online learner authentication: Verifying the identity of online users*, „MERLOT Journal of Online Learning and Teaching" 2009, No. 5 (2).

Acxiom; 2) Creating nine environmental variables within the administrator control panel, with values supplied by Acxiom; and 3) adding a pre-packaged Acxiom test prompt component to the screen, using existing ANGEL LMS functionality. Academic and system administrators determine the types of questions that will and will not be used to verify student identity, the number of attempts given to students, the time limitations for answering the challenge questions, and who is notified when there is a failure to properly authenticate.

Instructor Setup

Setting up Acxiom Identity-X to work with an assessment or other content item within the online course required instructors to either add a new assessment or content item or to click the modify settings link for an existing item. Once in the settings menu, as shown in Figure 1 below for the ANGEL LMS, the Acxiom integration adds a checkbox to enable the identity verification solution for that item and a pull-down menu to specify the random percentage of students in the course who will have their identity verified (1-100%). The third field (Acxiom Strategy) is set by the LMS Administrator.

Figure 1. New Assessment Menu with Acxiom Prompt (ANGEL LMS)



Source: Authors' own work

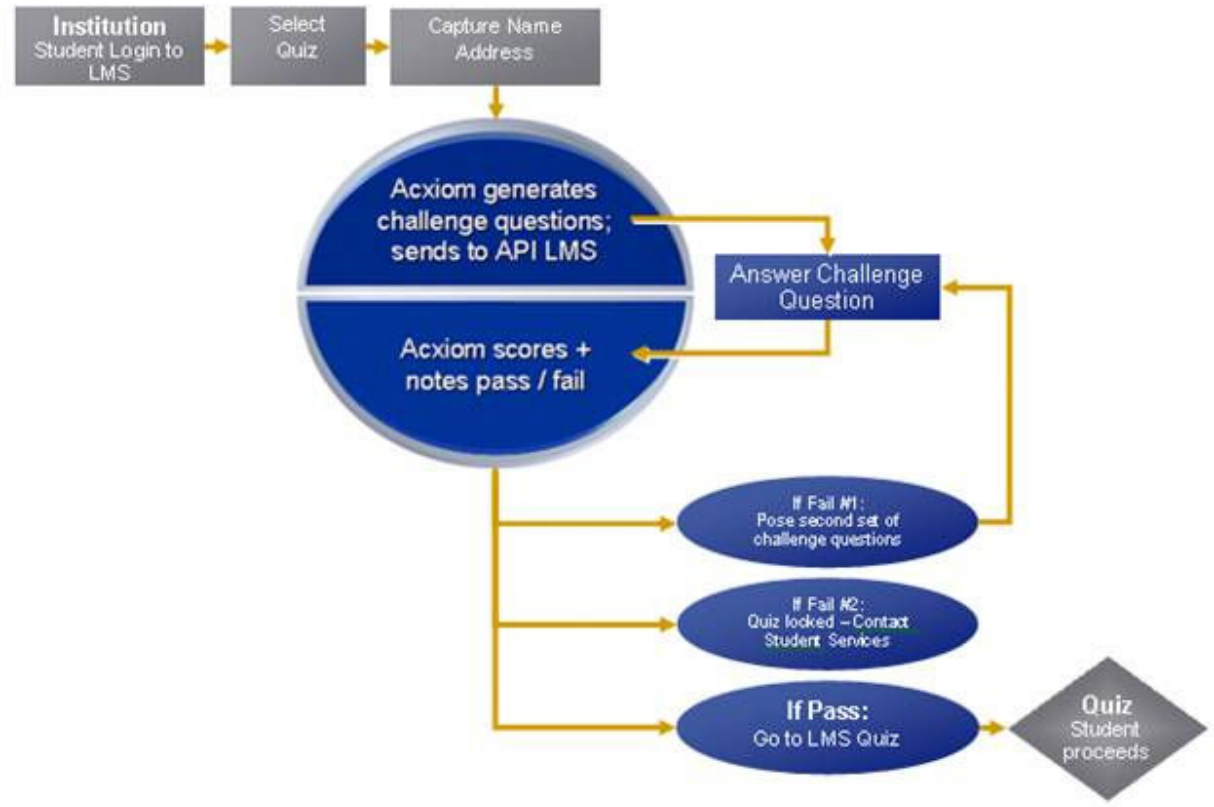
Implementation with Students

Ballie and Jorberg[17] illustrated the process of verifying student identity with Acxiom, as shown in Figure 2. below. When a student accesses an assessment or content item in which Acxiom has been enabled, he or she is prompted to enter the first and last name and address and the Acxiom system generates the challenge questions for students to answer. If students answer the questions

[17] Ibidem.

correctly, they are advanced immediately to the assessment or content item. If the student fails to answer the questions correctly, they may be given a second set of questions. If the challenge questions are not answered correctly or within the given time allotment, then a notification is sent to those parties selected by the academic administration.

Figure 2. Acxiom Student Identity Verification Process



Source: J. L. Ballie, M. A. Jortberg, Online learner authentication: Verifying the identity of online users, "MERLOT Journal of Online Learning and Teaching" 2009,No. 5(2)

Data Collection and Analysis

Data were gathered from students who participated in the pilot study, their instructors and the LMS Administrator. A six-item questionnaire was developed to assess student's perceptions regarding: 1) cheating in online versus face-to-face environments; 2) the effectiveness of the Acxiom solution for verifying online student identity; 3) whether the system is an effective

alternative to having students come to campus for testing; 4) whether the system would improve academic integrity; 5) whether the system respect study privacy and 6) whether the Acxiom solution is preferable to other methods of identity verification. Interviews with the course instructors and the LMS Administrator were undertaken to assess their experiences with system reliability and ease of use.

RESULTS

Instructors and LMS Administrator

Interviews with the course instructors found them to be in agreement that the Acxiom solution was extremely easy to set up and implement in their courses, involving only the determination of the course item to activate and clicking a checkbox. One of the instructors described it as "drop dead simple"[18]. Once the system was set up, the instructors found it to be maintenance-free.

The human resource leadership students received an explanation of the purpose of the identity verification system and student survey, accompanied by screen shots of the Acxiom system. The medical coding students received no prior warning, instructions or orientation to the system before they used it. There were no indications that the students who did not receive the prior orientation had any difficulty using the Acxiom system.

The administrator of the University's ANGEL Learning Management System declared the identity verification system implementation to be a very positive experience, due to the cooperation of the two vendors, Acxiom and ANGEL Learning. The system proved to be very reliable and Acxiom was responsive to call for assistance and information. Of all the verification solutions tested, Acxiom required the least amount of overhead and was the least expensive.

Students

Of the 112 students who participated in the identity verification field test, 85 completed the questionnaire, resulting in a return rate of 76%.

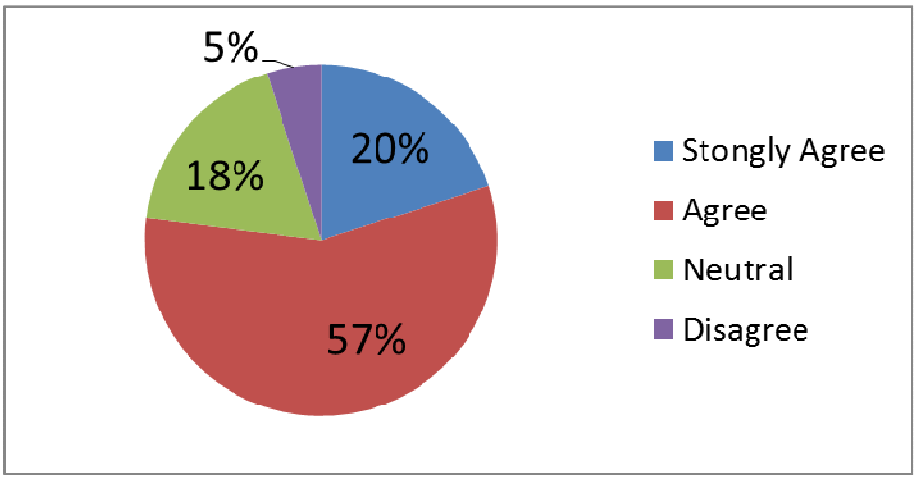
---

[18] A. A. Piña, B. R.Harris, op.cit.

Effectiveness of Acxiom Solution

When asked whether the Acxiom identity verification system is an effective way to verify online student identity, 77% of students answered in the affirmative, with only 5% of students disagreeing. 18% of students had no strong opinion either way. Results are displayed in Figure 3 below.

Figure 3. Acxiom is an Effective Way to Verify Identity (n=84)

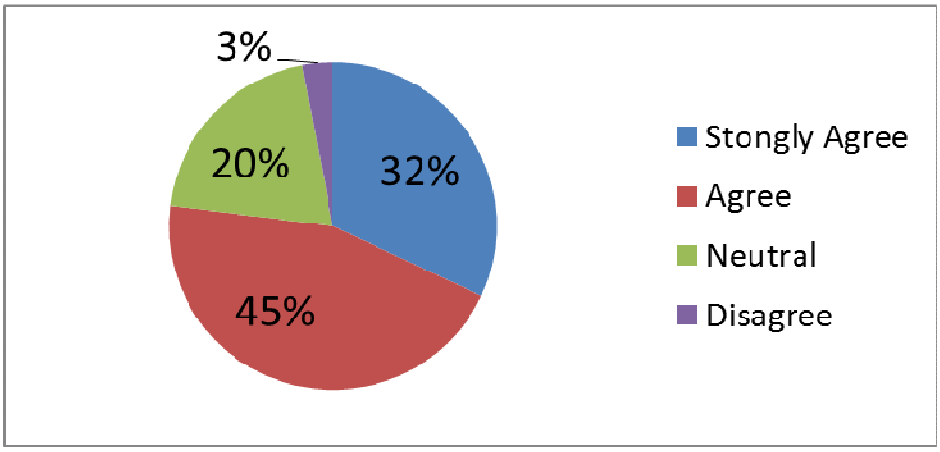


Source: Authors' own work

Alternative to Proctored Exams

Figure 4. shows the results when students were asked whether the Acxiom system was a good alternative to having students come to campus to take proctored exams. While 20% of students remained neutral, 77% of students agreed that Acxiom was a good alternative, while only 3% disagreed.

Figure 4. Acxiom is a Good Alternative to Taking On-Campus Proctored Exams (n=85)

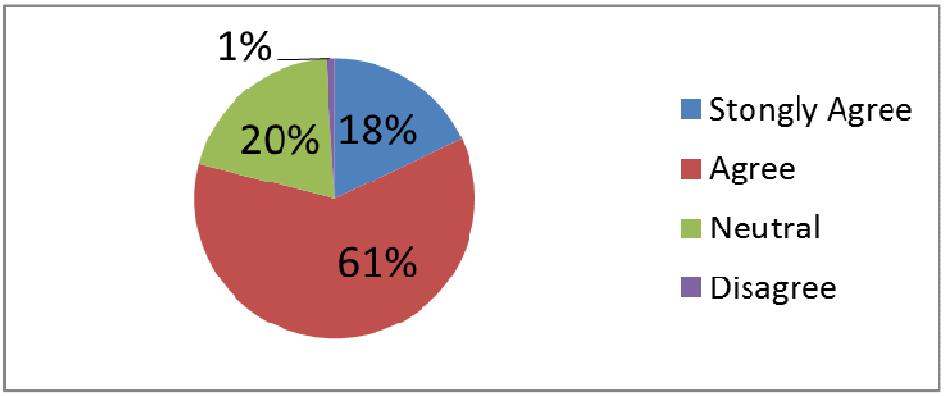


Source: Authors' own work

Respect for Student Privacy

One of the major concerns in this pilot implementation was whether asking personal questions to verify one's identity would be seen by students as an invasion of privacy—even when the questions were available through public databases. However, as demonstrated in Figure 5., when asked whether the Acxiom solution provided proper respect for student privacy, 79% of students answered in the affirmative, while a mere 1% (1 student) answered in the negative.

Figure 5. This System Provides Proper Respect for Student Privacy (n=85)

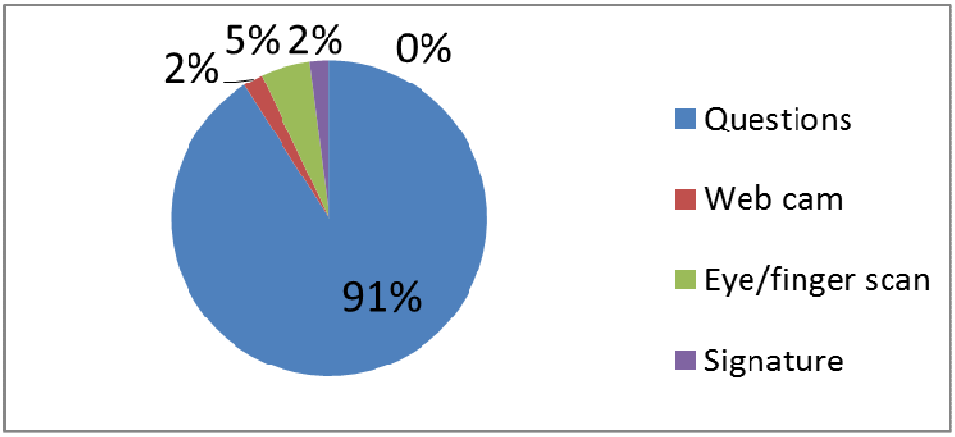


Source: Authors' own work

Preference for Identity Verification Solution

Student were asked to select their preferred method of identity verification among challenge questions (Acxiom), proctoring via webcam, biometric (eye/finger) scanning, signature/typing recognition or coming to campus to take exams. By more than a 9 to 1 margin, they chose Acxiom over all other solutions. None of the participants selected the option to come to campus to take exams.

Figure 6. I Would Rather the University Use the Following (n=84)



Source: Authors' own work

Unintended Benefit

An unintended benefit of the system occurred when one of the students was unable to receive challenge questions from the system. Acxiom investigated the student's public records and found the student listed on the Social Security Death Index and that her name was associated with social security number issued in the 1950s in Texas. The University verified the student's current contact information and social security number and Acxiom and the University were able to determine that the student was not engaging in an attempt to fraudulently college Title IV federal

financial aid, but was either the victim of identity theft or of a government clerical error, which placed her on the Social Security Death Index[19]. The student was contacted by the University and was able to resolve the issue with the Social Security Office.

Identity Verification vs. Cheating

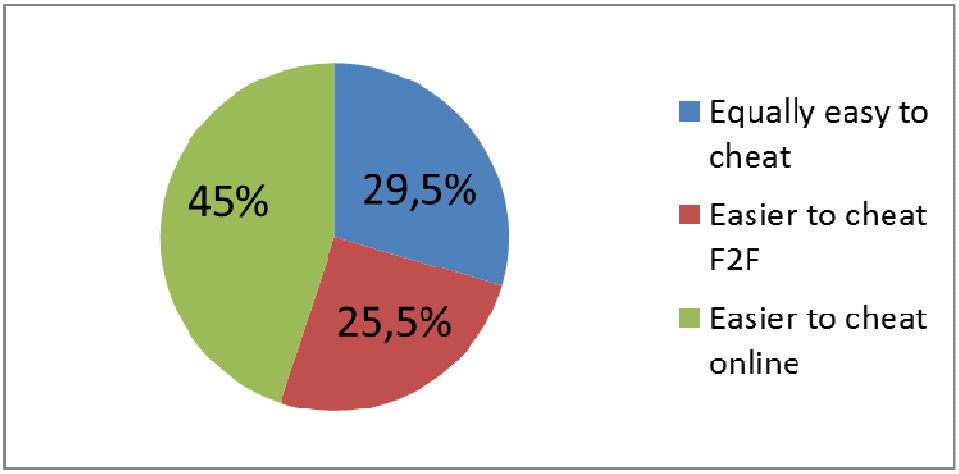
It should be noted that Section 495 of the Higher Education Opportunity Act and its subsequent interpretation and adaptation by the U.S. Department of Education and the regional accreditation agencies addresses only the verification of the identity of online students, rather than the prevention of cheating and plagiarism in online courses. In a study of assessment design and cheating in online courses, Harmon, Lambrinos & Buffolino[20] analyzed several studies on student perceptions of cheating in online versus face-to-face courses. In the oldest study[21], students believed cheating to occur more frequent in online courses. A more recent study[22] found reports of student cheating just as frequent in online and face-to-face courses, while the most recent study[23] found that students felt cheating to occur less frequently in online courses. The majority of students in Harmon, Lambrinos and Buffolinos' own study believed that the frequency of cheating was the same in face-to-face and online courses. The literature on cheating online versus face-to-face is inconclusive.

As part of this pilot study, students were asked whether it was easier to cheat in a face-to-face courses or an online course or if it was just as easy to cheat in either type of course. As shown in Figure 7, while 45 percent of the students agreed with the "conventional wisdom" that cheating is easier in online courses, 55 percent did not. One quarter of the students stated that it was easier to cheat in a face-to-face course and the remaining 30 percent stated that it was just as easy to cheat in either a face-to-face or an online course.

---

[19] M. A. Jortberg, 2010, op.cit.; A. A. Piña, B. R.Harris, op.cit.
[20] O. R. Harmon, J. Lambrinos, J. Buffolino, *Assessment design and cheating risk in online instruction*, "Online Journal of Distance Learning Administration" 2010, No. 13 (3).
[21] K. Kennedy, S. Nowak, R. Raghuraman, J. Thomas, S. F. Davis, *Academic dishonesty and distance learning: Student and faculty views*, "College Student Journal" 2000, No. 34 (2).
[22] T. Grijalva, C. Nowell, J. Kerkvliet, *Academic honesty in online courses*, "College Student Journal" 2006, No. 40 (1).
[23] D. Stuber-McEwen, P. Wiseley, S. Hoggatt, *Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom*, "Online Journal of Distance Learning Administration" 2009, No. 12 (3).

Figure 7. Ease of Cheating in Face-to-Face vs. Online Courses? (n=78)



Source: Authors' own work

INTERNATIONAL ISSUES

Accrediting agencies in the U.S. are overseen and authorized by the Council for Higher Education Accreditation (CHEA). In its 2008 report on the condition of accreditation, CHEA listed 41 of its accrediting agencies that accredited 385 non-U.S. institutions in 52 countries outside the U.S[24]. This may pose a challenge for identity verification systems that rely upon publicly available data, since the availability and regulation of personal data varies by country[25].

DISCUSSION/CONCLUSIONS

Although the utilization of a learning management system that incorporates a secure username and password currently satisfies the demands of the U.S. Government and the accrediting agencies, the leadership of Sullivan University Global e-Learning wished to adopt a system that

[24] Council for Higher Education Accreditation, *The condition of accreditation: U.S. accreditation in 2007*. CHEA Institute for Research and Study of Accreditation and Quality Assurance, Washington DC 2008.
[25] M. Neave, *International regulation of the publication of publicly accessible personal information*, „Privacy Law & Policy Reporter" 2003, No. 10, p. 120-122.

would keep them a step ahead of the minimum requirements. Of the various solutions available for verifying the identity of online students, Acxiom Identity-X was found to be the least invasive, required the least amount of configuration, did not require dedicated hardware or software, and was easiest and most cost effective to deploy. Instructors and system administrators found the Acxiom solution to be easy to set up and students found it to be an effective way to verify identity while respecting their privacy and preferable to other means of identity verification.

REFERENCES

- J. L. Ballie, M. A. Jortberg, *Online learner authentication: Verifying the identity of online users*, „MERLOT Journal of Online Learning and Teaching" 2009, No. 5 (2).
- N. Collins, *Woman sentenced to almost five years in federal prison for student loan fraud*, United States Attorney's Office, District of Nevada, Las Vegas 2006.
- Commission on Colleges, *Distance and correspondence education policy statement*, Southern Association of Colleges and Schools, Decatur 2010.
- Commission on Colleges, *Distance education and the principles of accreditation: Documenting compliance guidelines*, Southern Association of Colleges and Schools, Decatur 2009.
- Council for Higher Education Accreditation, *The condition of accreditation: U.S. accreditation in 2007*, CHEA Institute for Research and Study of Accreditation and Quality Assurance, Washington DC 2008.
- R. Epper, M. Anderson, L. McNabb, *Are your online students really the ones registered for the course? Student authentication requirements for distance education providers*, Western Cooperative for Educational Telecommunications, Boulder 2008.
- A. L. Foster, *A congressman questions the quality and rigor of online education*, Chronicle of Higher Education*"* 2006, No. 52 (30).
- T. Grijalva, C. Nowell, J. Kerkvliet, *Academic honesty in online courses*, „College Student Journal" 2006, No. 40 (1).
- O. R. Harmon, J. Lambrinos, J. Buffolino, *Assessment design and cheating risk in online instruction*, „Online Journal of Distance Learning Administration" 2010, No. 13 (3).

- Higher Education Opportunity Act (Public Law 110-315), 2008, http://ed.gov/policy/highered/leg/hea08/index.html.
- W. Hornbuckle, *Ringleader of $500,000 financial aid fraud scheme sentenced to prison*, United States Attorney's Office, District of Arizona, Phoenix 2010.
- M. A. Jortberg, *An Acxiom white paper: Methods to verify the identity of distance learning students*, Acxiom Corporation, Little Rock 2009.
- K. Kennedy, S. Nowak, R. Raghuraman, J. Thomas, S. F. Davis, *Academic dishonesty and distance learning: Student and faculty views*, „College Student Journal" 2000, No. 34 (2).
- M. Neave, *International regulation of the publication of publicly accessible personal informatio*n, „Privacy Law & Policy Reporter*"* 2003, No. 10.
- A. A. Piña*, How online diploma mills hurt e-learning*, „e-Mentor" 2009, No. 5 (32).
- A. A. Piña, *Online diploma mills: Implications for legitimate distance education*, „Distance Education" 2010, No. 31 (1).
- A. A. Piña, B. R. Harris, *On verifying online student identity,* Annual convention of the Association for Educational Communications & Technology, Anaheim, October 2010.
- V. Sampson, *Dear colleague: The higher education opportunity act,* Washington DC, Office of Postsecondary Education, U.S. Department of Education, 2008.
- C. L. Scheidenhelm, A. A. Piña, J. Corliss, *Authentication of online students: Current practices*, The annual Supporting Learning and Technology in Education (SLATE) Conference, Chicago, October 2009.
- D. Shieh, *Professors regard online instructor as less effective than classroom learning*, „Chronicle of Higher Education" No. 55, http://chronicle.com/article/Professors-Regard-Online/1519.
- D. Stuber-McEwen, P. Wiseley, S. Hoggatt, *Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom*, „Online Journal of Distance Learning Administration" 2009, No. 12 (3).

Information about the authors

Anthony A. Píña is Dean of Online Studies for the Sullivan University System and has 23 years experience in the field of instructional technology and distance learning. He is the author of the book "Distance Learning and the Institution" and serves on the Executive Board of the Association for Educational Communications and Technology (AECT), and on the Editorial Board of the Quarterly Review of Distance Education.

Larry Bohn serves as Associate Dean of Outcomes Management and Coordinator of the Online Medical Coding program for the Sullivan University System. He has over 30 years experience developing and delivering training in the academic, corporate, and government arenas and holds several technical certifications. Larry has taught face-to-face and online classes at community college, university and seminary settings.

Jeff Lyons is Learning Management System Administrator for Sullivan University System Global e-Learning. Prior to coming to Sullivan, Jeff was a Principal with Mercer Human Resource Consulting as the Lead of Software Implementation.