

An Acxiom White Paper

Experiences Verifying the Identity of Distance Learning Students

3rd Annual Report on Identity in Distance Learning

by Michael Jortberg,
Acxiom Corporation



Table of Contents

Background1

Integrity in Online Education2

Higher Education Industry Regulations4

Experiences with Challenge Questions6

Case Studies7

Risks Drive Identity Requirements8

Preparedness and Best Practices8

Conclusion10

Suggested Reading10

About Acxiom11

The education industry is exploring and improving strategies to verify the identities of distance learning students. Accreditors require institutions to document their processes for ensuring integrity of their online courses by verifying the identities of online students. A growing approach is to strengthen students' user IDs and passwords by adding new processes and technology to increase academic integrity and ensure proper use of federal student aid. Assessing an institution's risk for online academic integrity and student aid fraud helps guide the adoption of student identity solutions.

Background

Distance education is transforming the United States Higher Education model. Just as the music and publishing industries are being reshaped, new education models have taken hold and traditional institutions are adapting to current consumer demands. The for-profit education sector and community colleges are experiencing significant online education enrollment growth to meet consumer demand for education in a down economy.

Along with growth comes quality concerns related to two areas: academic integrity and criminals targeting online education programs for student aid fraud.

To address these concerns, a new federal policy to verify the identity of online students is being implemented. The U.S. Department of Education's recognized accreditation agencies now require institutions to document how they comply with a new federal policy requiring identity verification of online students. This has always been a common concern in distance education — how do you know who's doing the work for the credit?

Integrity in online education

Like clockwork, there are consistent media stories and cases about cheating in education. In 2008, University of California San Diego published its second *Annual Report on Academic Integrity*¹, which states:

“If students perceive wide-spread cheating and dishonesty, even the most honest student may find herself cheating under the impression that she has no choice. Or, if students do not hear the University publicly condemn unethical behavior or do not see the University supporting ethical behavior, then even the most integrous student may find himself cheating under the impression that the behavior is no longer unacceptable.”

In 2009, a number of incidents specific to online learning demonstrated how the current technology of user ID and password failed to protect the interests of taxpayers, the institutions, faculty and students. In June, 65 people were indicted in a student loan scam where a ringleader would enroll and log in as others to fraudulently obtain student aid funds.² In July, a police investigation revealed college staff routinely shared user IDs and passwords to enable students to pass exams.³ In January 2010, The National Collegiate Athletic Association (NCAA) published a case in which user ID sharing enabled academic integrity violations:

“The former assistant coach was clearly assigned academic oversight responsibilities for the men’s basketball program. In that capacity, he obtained all of the men’s basketball student-athletes’ online academic account IDs and passwords at the beginning of each academic year. This enabled him to log on to the institution’s Internet system posing as the student-athletes. His access included, but was not limited to, class schedules, unofficial transcript and financial information. Additionally, if a student enrolled in an online course, the ID and password were used to access the course and to participate in required online chats.”⁴

In October 2009, the U.S. Department of Education’s acting Inspector General testified about integrity in online learning before a Congressional hearing of the Committee on Education and Labor Subcommittee on Higher Education, Lifelong Learning, and Competitiveness in the House of Representatives. Mary Mitchelson testified that the Inspector General’s staff regularly confronts fraud in distance education. The DOE IG has conducted 29 investigations related to distance education since 2005, 19 from the past two years and more since Mitchelson’s testimony. She outlined four key issues in distance education that need to be addressed through policy changes:⁵

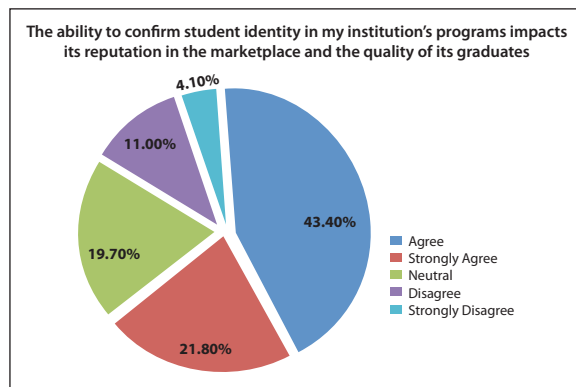
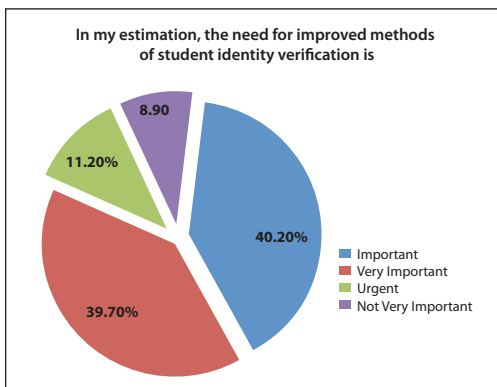
- Is the student who they say they are?
- Is the student securing aid for instruction or is student aid used elsewhere?
- Is the student receiving the correct amount of aid?
- If a student drops out, how much instruction did the student receive and therefore how much aid should be repaid?

Congress has already mandated that improvements be made to increase the integrity of online higher education. Some faculty who teach distance education courses agree with Congress. In an August 2009 faculty survey by researchers at Kaplan University⁶, instructors were asked for their opinions about the need to improve methods of student identity verification.

When asked about importance, more than 92% felt confirming identity was important, very important or urgent. Below are responses to the question “In my estimation, the need for improved methods of student identity verification is...”

Also from the Kaplan study, faculty feel improving identity in distance education improves the reputation and credibility behind their institutions’ degree — proven by their response to this question: “The ability to confirm student identity in my institution’s programs impacts its reputation in the marketplace and the quality of its graduates:”

Important	Very Important	Urgent	Not Very Important	Agree	Strongly Agree	Neutral	Disagree	Strongly Disagree
168	166	47	37	181	91	82	46	17
40.20%	39.70%	11.20%	8.90%	43.40%	21.80%	19.70%	11.00%	4.10%



Dr. Barbara Beno, President of the Accrediting Commission for Community and Junior Colleges, is a leader in the higher education accreditation field. She weighed in on the credibility of distance education when she posted this comment in response to a student aid fraud case documented in *The Chronicle of Higher Education*:

“In addition to the financial aid fraud described in this article, there is a significant issue of institutional integrity. If a ‘fake’ student can sign up for credits so readily, can a ‘fake’ student also ‘earn’ credits easily? Arguing that there can be fraudulent practices in large lecture courses, and that distance education should not be required to institute more security than is presently required, is not wise if the higher education community wishes to encourage public confidence in online education. All higher education institutions need to work to ensure the quality and integrity of ALL of their forms of educational delivery systems. Without necessary oversight to assure integrity and quality, the greater ‘access’ provided through distance education may result in a substandard reputation for the institutions and the students who complete on-line programs and courses.”⁷

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.⁸

U.S. accreditation agencies now question how institutions with distance education programs verify the identity of distance learning students. Specifically, the Higher Education Opportunity Act (HEOA), which was signed August 14, 2008, states, “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.”⁹ In the Joint Explanatory Statement of The Committee of Conference, Congress stated the current technology (as of mid-2008) of user IDs and passwords are sufficient, but that, “As technology develops over time, the Committee anticipates that additional identification technologies will become more sophisticated, less expensive and more mainstream.”¹⁰

As of early 2010, many regional accreditors pose questions to accredited institutions regarding exams.

“When examinations are employed (paper, online, demonstrations of competency, etc.), they take place in circumstances that include firm student identification. The institution otherwise seeks to assure the integrity of student work.”¹¹

- If proctoring is used, what are the procedures for selecting proctors, establishing student identity, assuring security of test instruments, administering the examinations, and assuring secure and prompt evaluation?
- If other methods are used to identify those who take the examination, how is identification firmly established? How are the conditions of the examination (security, time limits, etc.) controlled?
- Does the institution have in place effective policies and procedures to assure the integrity of student work?

As Congress expected, in the 18 months since the HEOA was signed, the market has developed new technologies to meet the needs of concerned faculty. In 2008-2009, new technology solutions have been adopted and are now generally available to improve upon user ID.

These solutions are being used in addition to current academic integrity tools, such as plagiarism detection databases, secure web browsers, encrypted test question banks, and publicizing policies for cheating and ethical violations. The following table outlines categories of solutions currently being implemented.

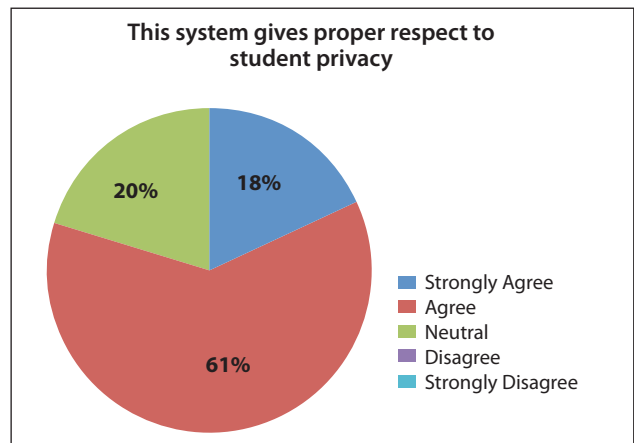
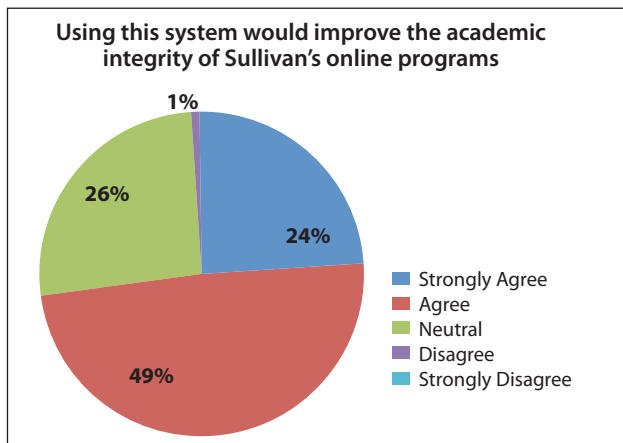
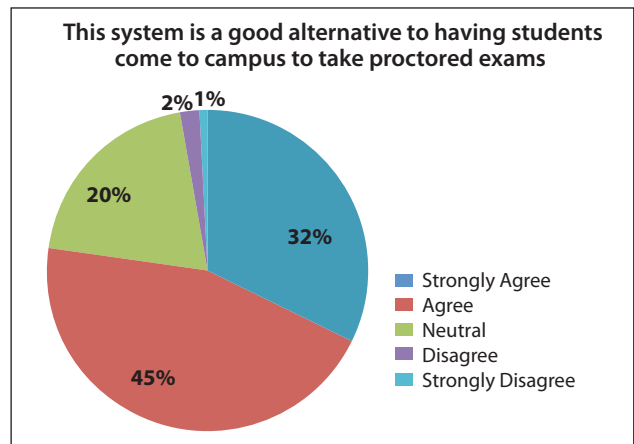
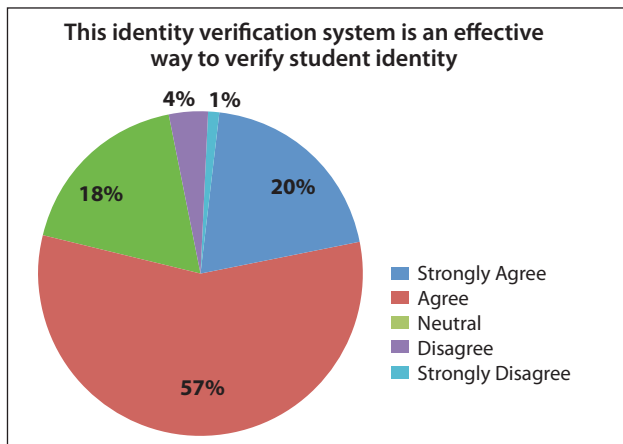
	Challenge Questions	Web Proctor	Biometrics/ Special Hardware	In Person Proctored Exam
Methodology	Challenge questions based on third-party data.	Audio and video conference proctoring via webcam. Screen monitoring service with live, certified proctors.	Unique typing style or fingerprint plus targeted recording of student in exam via webcam.	Face to face with government or institution issued identification.
Applications	Any assessment may be protected with random settings for low- or high-value assessments.	Typically high-value assessments such as midterms and finals. Also applicable to placement exams or industry certifications.	High-value assessments, such as finals, capstone assessments, placement exams or industry certifications.	Typically high-value assessments such as midterms and finals. Also applicable to placement exams or industry certifications.
Student Enrollment or Registration Process	None required. Supports walk-up students.	Acquire webcam upon enrollment. Student schedules exam with proctor via online scheduling system.	Capture fingerprint, typing samples or digital pictures. Student and device registration for student's Windows PC. May require student signature on consent form.	Proctor approval process. May require pre-registration of exam time, location and proctor.
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.	Instruct students to schedule exams with proctor. 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.	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.
Pricing Model and Additional Institution or Student Costs	Per transaction pricing, no additional costs.	Per exam or hour. Purchase of a standard, sound-equipped webcam.	Startup and often per exam. Server software and database applications. Shipping costs for special device. May require specialized webcam or Windows PC software.	Per exam or hour. Student travel time, child care, and time away from work. Proctor quality assurance process.
Limitations	As of early 2010, primarily a U.S.-only solution.	Addressing paradigm shift with hesitant faculty.	Extensive faculty and student training and startup effort. Windows required.	Very high administrative costs; Limited test center hours.

Experiences with challenge questions

During 2009, institutions began using the Acxiom Identify-X™ challenge questions to verify students' identities. Feedback from students, faculty, IT administrators and distance education leaders was very positive. After thousands of identity verification transactions, Acxiom users reported no privacy concerns and no significant deployment challenges. One institution was fully operational in less than two hours. At Sullivan University in Louisville, 85 students responded to a survey about identity verification. Sullivan staff concluded challenge questions were best suited for their programs and students:

	This identity verification system is an effective way to verify student identity.	This system is a good alternative to having students come to campus to take proctored exams.	Using this system would improve the academic integrity of Sullivan's online programs.	This system gives proper respect to student privacy.
Strongly Agree	20%	32%	24%	18%
Agree	57%	45%	49%	61%
Neutral	18%	20%	26%	20%
Disagree	4%	2%	1%	0%
Strongly Disagree	1%	1%	0%	0%

Sullivan University student feedback



Given the choice, I would rather that Sullivan University use the following method to verify online student identity:

Having students answer questions (i.e. the system that I just used)	91%
Having students use a web cam so that a proctor can see them	2%
Having students' fingerprints or eyes scanned using a scanner	5%
Having students' signatures or eyes scanned using a recognition program	2%
Having students come to campus to take exams (live proctor)	0%

Case studies

Below are three case studies from identity projects conducted by Acxiom in 2009.

Case 1: Student Aid Fraud

For this state system, Acxiom helped identify a group of out-of-state online students who appeared to be committing student aid fraud. Upon review of the students' enrollment data, we learned that many students shared names, addresses and phone numbers. This alone was cause for alarm. Further comparison against the student records to the Acxiom Identify-X system showed these individuals had a high number of inaccurate Social Security numbers, dates of birth, addresses and phone numbers. We found that one student submitted a prison address and a second a nightclub as their residence. This inexpensive methodology to verify a student's identity supports not only the HEOA identity provisions but also Federal Trade Commission red flag programs to detect and prevent many forms of identity theft. The Department of Education's Inspector General testified to Congress about these types of scams on October 14, 2009.¹²

Case 2: "Dead" Student Taking Exam

In this case, an online school in the Southeast had an out-of-state 24-year-old student who could not receive challenge questions. Upon investigation, Acxiom learned the student was listed on the Social Security Death Index. Together with the institution, we immediately verified her name, address, phone, SSN and date of birth to ensure she was not committing Title IV student aid fraud. We learned she was the victim of identity theft. Her name was linked to a dead individual's SSN from the 1950s in Texas. The student services department proactively notified the student of the issue.

Case 3: MBA Fails Identity Test

This online Masters of Business Administration program posed four challenge questions to all students enrolled in a series of courses. The integration to their custom learning management system (LMS) identified which students should receive challenge questions and then allowed them three minutes to respond. This student missed all four questions. Upon review, the institution notified faculty and administration to be aware of this student and to closely monitor his work in the future.

Risks drive identity requirements

When focusing on academic integrity, academic leaders should review assessment strategies in their online courses to help decide their approach to student identity. Acxiom customers concluded that courses with online assessments and little instructor interaction are the best candidates for frequent random student identity verification. Advanced-level courses with face-to-face instruction, threaded discussions, term papers or projects need less frequent identity verification.

Just as assessment types differ across lower- and upper-level undergraduate and graduate programs, identity verification technology and policies should match the risk associated with the assessment. Many large 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.

When focusing on student aid fraud, in-person registration or secure and "identity verified" processes can deter fraudsters from entering a program. Additional data mining techniques can spot relationships between students who may be working together to commit fraud. Comparing information in the institutional student information reports (ISIRs) and a school's enrollment records as well as monitoring for red flags, such as invalid Social Security numbers and falsified directory information, can help detect and prevent student aid fraud in online programs.

Preparedness and best practices

We offer the following checklist to institutions evaluating student identity programs:

- Educate faculty and staff about your national, regional or specialized accreditors' requirements for student identity in online courses.
- Document online student identity process for annual accreditation survey or new program reviews. Determine what evidence is required to demonstrate that your institution verifies student identity in online courses.
- Ask the following questions:
 - What are our processes and technology to firmly ensure identity in online programs, courses and assessments?
 - Are we balancing both process improvements and technology to address this issue?
 - Are we over- or under-relying on process or technology, thereby creating an opportunity for fraud?
- Determine your risks for academic integrity in online courses. Ask "If students or employees share user IDs and passwords, can they circumvent my institution's identity controls and policies?"

Highest Risk Courses	Medium	Lowest Risk Courses
<p>Fully online courses with little or no student/faculty interaction. Objective assessments delivered online without proctor.</p> <p>Online assessments with high stakes riding on the outcome, such as athletic program participation.</p>	<p>Hybrid or web enhanced courses with low or medium student/faculty interaction. Objective or subjective assessments delivered online without proctor.</p>	<p>Face-to-face instruction with proctored or no online assessments. Online course with high student/faculty interaction.</p>

- Determine your risks for student aid fraud in online courses. Ask “If students or employees share user IDs and passwords, can they circumvent my institution’s identity controls and policies?”

Highest Risk Courses	Medium	Lowest Risk Course
<p>Students with state, federal or private grants in fully online course.</p> <p>No face-to-face component or a self-paced program.</p> <p>Fully online enrollment and course delivery.</p> <p>Course participation verified by checking activity logs and little to no student interaction.</p> <p>No face-to-face requirements.</p> <p>No FTC red flag or identity technologies beyond user ID.</p> <p>High concentration of students in remote or out-of-state locations.</p>	<p>Students with grants in fully online course with little face-to-face component.</p> <p>Flexible face-to-face requirements.</p> <p>Course participation verified by faculty beyond system logins and activity.</p> <p>No red flag or identity technologies beyond user ID.</p>	<p>Web enhanced or face-to-face courses with little loan or grant funding.</p> <p>Face-to-face or webcam interaction periodically required.</p> <p>Courses rely on face-to-face proctored assessments with reliable photo ID.</p>

Conclusion

Many industries that deliver online services have developed processes and deployed technology for ensuring integrity. Higher education is now increasing academic integrity and preventing student aid fraud in online education by implementing identity verification in distance learning programs. To adopt best practices to prevent misuse of financial aid funds and improve program quality, institutions should evaluate their online programs, assessment policies and student loan risk profile to match the right level of identity verification to ensure the student who enrolls is also the student who does the work and receives course credit.

Michael Jortberg is Higher Education Leader at Acxiom Corporation. He can be reached at Michael.Jortberg@acxiom.com.

Suggested reading

- 1st Annual Report MERLOT JOLT Verifying the Identity of Online Users
http://jolt.merlot.org/vol5no2/ballie_0609.htm
- 2nd Annual Report Acxiom white paper, January 2009, “Methods to Verify the Identity of Distance Learning Students”
http://www.acxiom.com/SiteCollectionDocuments/website-resources/pdf/White_Papers/AC-0031-09_DistanceLearningStudentsWP.pdf
- Best Practices: WCET’s Strategies to Promote Academic Integrity in Distance Education
http://wiche.edu/attachment_library/Briefing_Paper_Feb_2008.pdf.
- Academic Integrity in Online Education by The Sloan Consortium
<http://www.sloan-c.org/node/1495>
- Higher Learning Commission’s Best Practices For Electronically Offered Degree and Certificate Programs http://www.ncahlc.org/download/Best_Pract_DEd.pdf
- Ensuring Student Eligibility Requirements for Federal Aid
<http://edlabor.house.gov/hearings/2009/10/ensuring-student-eligibility-r.shtml>

About Acxiom

Acxiom provides marketing and risk mitigation consulting services and technology solutions in higher education. Acxiom is a participating member of Educause and WCET.

Identity and Privacy

- Verify identity of distance learning students.
- Comply with Federal Trade Commission “red flag” policies.
- Background screening to reduce hiring and admissions risk while hiring academic staff, third party contractors and certain students populations.

Admission Marketing

- Create an accurate and enriched view of potential students.
- Maximize admissions strategies and current and comprehensive prospective student data enrollment marketing technologies.
- Segment student and alumni data according to behaviors that reflect the most up-to-date status of U.S. households and life stages.
- Analytics: Develop a precise quality lead portrait and contact strategy through predictive modeling.

Alumni Relations

- Stay in touch with alumni for fund raising and community development with our partner, Harris Connect.

IT Services

- Mainframe outsourcing and hosted storage, network and server management services.

¹ University of San Diego Academic Integrity 2007-2008 Annual Report http://academicaffairs.ucsd.edu/ug-ed/academicintegrity/AI_2007-2008_Report.pdf

² 65 indicted in student loan fraud against Rio Salado College
<http://www.azcentral.com/community/peoria/articles/2009/06/24/20090624loanfraud0624-ON.html>

³ 'Gross academic fraud' at UTB-TSC rocked Office of Distance Education
<http://www.brownsvilleherald.com/news/online-100590-utb-employees.html>

⁴ NCAA Georgia Southern University Public Infractions Report, January 20, 2010
<http://www.ncaa.org/wps/wcm/connect/f4ebf400411cfa44afe7ff122174eb00/20100120+Georgia+Southern+Infractions+Report.pdf?MOD=AJPERES&CACHEID=f4ebf400411cfa44afe7ff122174eb00>

⁵ Ensuring Student Eligibility Requirements for Federal Aid
<http://edlabor.house.gov/hearings/2009/10/ensuring-student-eligibility-r.shtml>

⁶ Student Identity Verification and the Higher Education Opportunity Act: A Faculty Perspective
http://itdl.org/Journal/Aug_09/article05.htm

⁷ Online Scheme Highlights Fears About Distance-Education Fraud
<http://chronicle.com/article/Online-Scheme-Highlights-Fears/63517/>

⁸ The Fundamentals Of Accreditation
http://www.chea.org/pdf/fund_accred_20ques_02.pdf

⁹ ACE Analysis of Higher Education Act Reauthorization
www.acenet.edu/e-newsletters/p2p/ACE_HEA_analysis_818.pdf

¹⁰ Joint Explanatory Statement Of The Committee Of Conference
http://help.senate.gov/Hearings/2008_07_29_E/Statement_of_Managers.pdf

¹¹ Best Practices For Electronically Offered Degree and Certificate Program
http://www.ncahlc.org/download/Best_Pract_DEd.pdf

¹² Ensuring Student Eligibility Requirements for Federal Aid
<http://edlabor.house.gov/hearings/2009/10/ensuring-student-eligibility-r.shtml>

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

1.888.3ACXIOM

