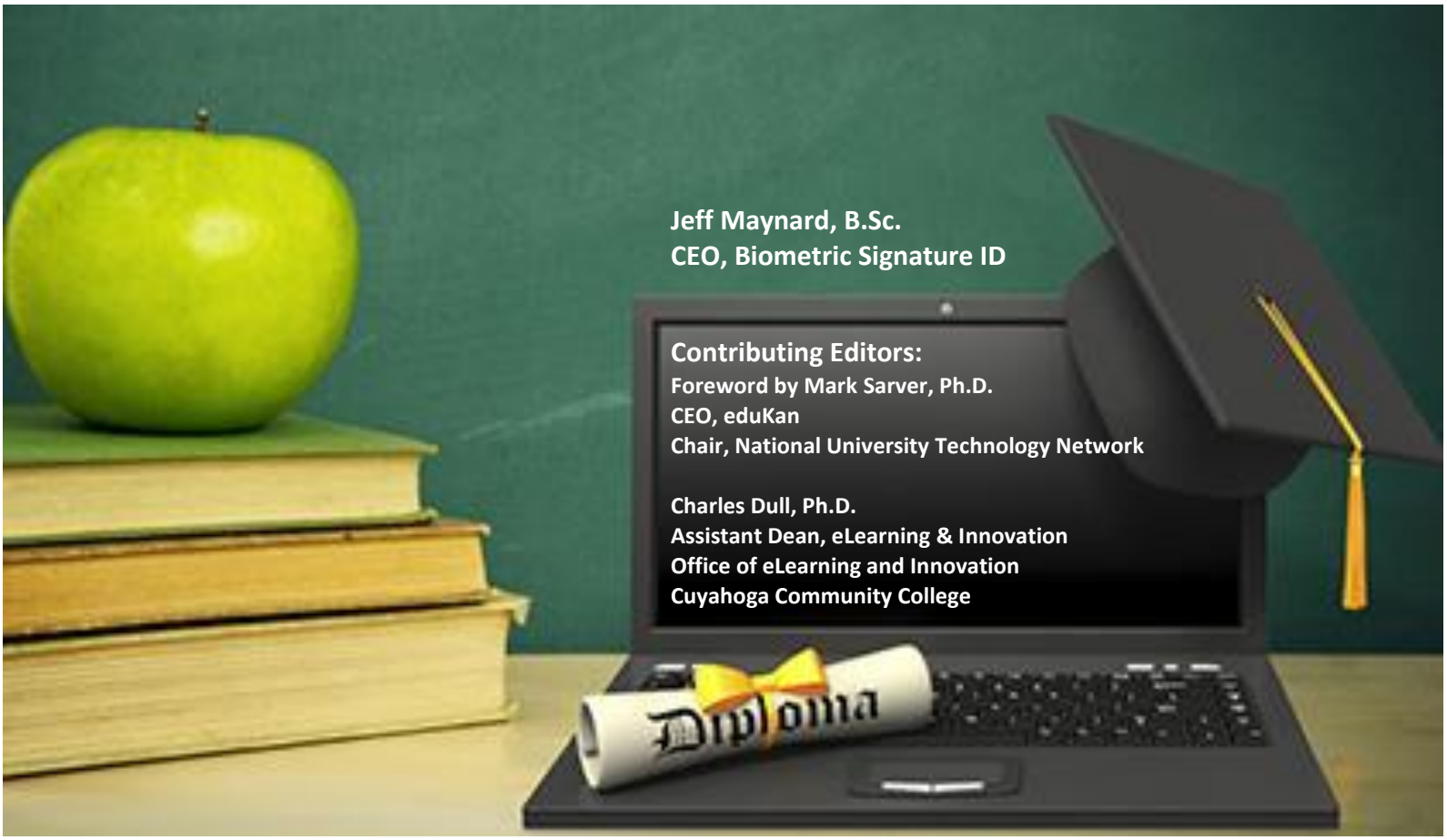
Student ID Verification:
What Institutions Need To Know
- White Paper -



Jeff Maynard, B.Sc.
CEO, Biometric Signature ID

Contributing Editors:
Foreword by Mark Sarver, Ph.D.
CEO, eduKan
Chair, National University Technology Network

Charles Dull, Ph.D.
Assistant Dean, eLearning & Innovation
Office of eLearning and Innovation
Cuyahoga Community College

BSI

BIOMETRIC SIGNATURE ID

Table of Contents

Foreword

As an administrator in higher education, I am charged with creating an innovative online learning program. I am continually searching for new and better ways to engage students, improve learning and ensure quality while fulfilling our mission to be accessible and affordable. I was delighted to partner with Biometric Signature ID four years ago and our team continues to work hand-in-hand with the Biometric Signature ID team to develop enhanced and expanded products.

I first met Jeff Maynard, President and Founder of Bio-Sig, at a conference where I was looking for a solution to physical proctoring. From that initial meeting, I could tell his was the kind of innovative company I wanted to work with to develop our student identification and verification process to extend beyond the physical testing center. In addition to the work they are doing in the higher education space, Bio-Sig ID has been chosen by the White House to help the government address online fraud; they have been selected as one of the Top 20 Most Promising Ed Tech Companies by CIO REVIEW and have become leaders in remote student identification and verification.

eduKan, a consortium of community colleges in Kansas, faced a daunting task of managing the proctoring for 4,000 geographically dispersed online students. The staff and faculty of eduKan was spending hours managing the paperwork, coordinating proctors, dealing with students who forgot to arrange a proctor or searching for missing paperwork. The frustrations for the student were just as significant; arranging the proctor, ensuring the paperwork was processed correctly, physically going to the proctoring facility, arranging babysitters for children, just to name a few. The list of obstacles to student success continued to mount.

Searching for a technology-based solution was just as frustrating. Part of eduKan's mission is to be accessible, convenient and affordable and most solutions either required expensive equipment to be rented or purchased by the student or the solutions were simply too cost prohibitive. The implementation of Biometric Signature ID quickly emerged as the ideal solution. After a beta test, eduKan has now fully implemented Biometric Signature ID into the learning management system and can uniquely identify every student within the system. Not only can we ensure student authentication and discourage cheating, we can also state unequivocally that the process is not a barrier or burden to the vast majority of students who are not cheating. And all at a cost that allows eduKan to continue to fulfill its mission of accessibility, convenience, and affordability.

Although we were initially using Bio-Sig ID to address academic integrity, we have since learned that there are applications as a financial aid compliance tool. In addition to the standard requirement of login and submission of an assignment within the first week of class, we require all students to authenticate using Bio-Sig before we certify the student and disburse financial aid. The ability to validate and quickly identify potentially fraudulent students has made a positive impact on reducing financial aid fraud cases reported at our consortium-member colleges. Additionally, eduKan has taken the lead in developing a statewide communication tool allowing financial aid staff from all 19 community colleges to share important information on potentially fraudulent situations. This serves to effectively keep a Pell runner or straw student from simply choosing another one of Kansas' community colleges.

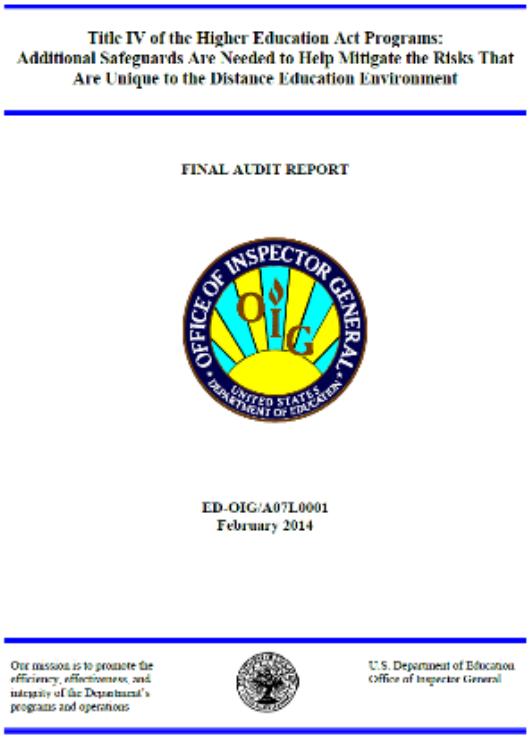
Thousands of honest students have taken classes from eduKan since we started the partnership with Biometric Signature ID using an authentication system that is neither intrusive nor a barrier to their success. We also feel that our exposure to fraudulent activities have decreased as potential scammers are being exposed. And for those that try to commit Pell fraud, we stand ready, armed with Biometric Signature ID data and evidence to stop them.

Jeff has compiled an informative update of the current environment for student verification and has combined the knowledge of years of experience working with institutions. Many of the findings from the Office of the Inspector General, Department of Education show that simply requiring a username and password will not be enough to ensure the student is legitimate and valid. Additionally, accrediting agencies are looking to strengthen their requirements for student authentication. We are pleased to have partnered with Biometric Signature ID and feel that we are well prepared to comply with any new regulations that might jeopardize online programs at institutions that are not prepared.

Dr. Mark E. Sarver
Chief Executive Officer, eduKan
Chair, National University Technology Network (NUTN)

1.0 Student ID Verification Online: What Institutions Need to Know:

Online education does not require the physical presence of a student. This has created a fertile ground for identity fraud including academic dishonesty and financial aid fraud. Learning management systems for example use only a Pin or password to provide access to a students' course materials and gradable events. These identity verification methods are no longer enough because they are too easily shared/accessible to non-registered students.


Title IV of the Higher Education Act Programs:
Additional Safeguards Are Needed to Help Mitigate the Risks That Are Unique to the Distance Education Environment

FINAL AUDIT REPORT

ED-OIG/A07L0001
February 2014

Our mission is to promote the efficiency, effectiveness, and integrity of the Department's programs and operations

U.S. Department of Education
Office of Inspector General

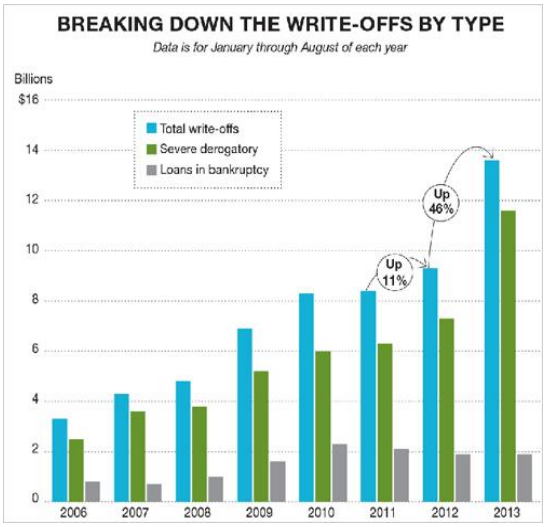
According to the *Office of Inspector General (OIG), Department of Education Final Audit Report February 2014,* "A secure login and passcode ensure only that someone logging in to a course is using the same login and passcode assigned to the person who enrolled. Without effective enrollment processes at a school, a login and passcode do not ensure that the person is enrolling under a valid name and intending to obtain an education."

How did we get here?

The use of Pins and passwords as our means of security has fostered the following environments.

- **Easy for others to access and complete your work:** As reported in the Chronicle Review, the Shadow Scholar admitted he has attended 36 online universities/colleges to complete essays and other homework activities including online chats. His company of 50 staff cannot keep up with the demand from students. He states that "Somebody in your classroom uses a service that you can't detect, that you can't defend against, that you may not even know exists". (Dante)
- **Over 28M web sites offer services:** At last count over 28M web sites exist to provide academic services for students for a fee. (Google search for "essay writing services for students" 1/2/2015). One version of "Take-my-exam.com" called AllHomework.net boasts, "Just let us know what the exam is about and we will find the right expert who will log in on your behalf, finish the exam within the time limit and get you a guaranteed grade for the exam itself."
- **You can buy your education:** Exam taking generally costs $250.00 to $500.00, online chats and participation range $60-100/week, essay pages range from $10/page to $30.00 per page. For someone to take your whole course the costs range from $600.00 - $3,000.00 (data on file).
- **Financial aid fraud is rampant.** Fraud rings- large, loosely affiliated groups of criminals who seek to exploit distance education programs are becoming a fixture in distance education especially in schools offering lower tuition. Because of the virtual nature of courses, fraud ringleaders have been able to use the identities of others (with or without their consent) to target distance education programs to fraudulently obtain Federal student aid. The OIG even has a web site for sharing the details of this fraud: http://www2.ed.gov/about/offices/list/oig/ireports.html
    a. One large for-profit in 2014 stated publically (data on file) they have seen over 1,000 fraud rings and report over 300 students per month to the Office of Inspector General for fraud.
    b. Axia College, a two-year program of the for-profit University of Phoenix, has identified 750 fraud had identified 750 fraud rings involving 15,000 people. Four staffers work full time to verify students' identities and weed out scammers and Pell runners (Joanne).

c. In 2005, the OIG had opened 16 distance education fraud ring investigations; as of August 1, 2011, the OIG had opened 100 (Testimony of Inspector General Kathleen S. Tighe).
d. More than 34,000 participants in crime rings improperly received federal student aid last year (2012), up 82% from 2009, the department's inspector general estimated this month. Improper payments through the federal student-loan program more than doubled last year from the year before to $614 million (Mitchell).
e. "In January 2013, we provided the Department with the results of our risk analysis related to student aid fraud rings, which estimated a probable loss of more than $187 million in Federal student aid funds from 2009 through 2012 as a result of these criminal enterprises." (Office of Inspector General)
f. Roughly $829 million in Pell grants in the fiscal year ending September (2012) were "improper payments," which includes fraud and disbursements due to clerical errors (Mitchell).



Interesting, could these fraud cases be contributing to the mounting student debt crisis where write-offs jumped 46% during the first eight months of 2013 compared with the same period in 2012?

It is difficult to obtain repayment of loans from straw students, or fraudsters who are difficult to track down after receiving money.

What is the percentage of fraud?

The National Association of Student Financial Aid Administrators, said it has flagged 126,000 applicants, about 1% of all those seeking aid for the 2013-2014 school year (Mitchell). These are the fraudsters who were identified, but how can we account for the ones not caught/identified? One way to analyze this is If we do the math using the 2012 Pell Grant appropriations of $22.8B/$1B improper payments. In this way the number edges closer to a 4% fraud rate (Delisle). "On a per student basis, using the case of a well-known college in Arizona, where 65 individuals were charged in a federal financial aid fraud resulting in the loss of over $530,000 from Stafford loans and Pell grants (United States Attorney District of Arizona), the average fraud per student was $8,153.00." Whatever the final or most accurate number is – it is still way too high and is a big issue we need to deal with for online education regardless of which party is running the government.

Could financial aid fraud be as high as 4%?

If these numbers hold true it means that institutions are at risk by up to 4% of their financial aid revenue! The institution risks these monies as they may have to pay tuition back without getting any reimbursement from students who drop/fail on purpose. You cannot determine whether they stole the money because you cannot catch them after they disappear. This subsequently increases the institutions' default rates.

What does financial aid fraud do to your budget – case report:

It creates a deficit! This can cost jobs, create cost cutting measures such as benefit reductions and force tuition increases. Here's an example that is excerpted from the Dearborn News Herald:

> *"Henry Ford Community College expects to raise tuition rates about 7 percent next year as it looks to balance its budget and tries to control costs related to students milking federal student loan programs." Board Treasurer James Schoolmaster at HFCC said one issue hurting the college is student misuse of federal loans. Twenty percent of tuition revenue will need to be returned next year because students never really attended or failed all their classes.*
>
> ***HFCC is expecting to have to pay back about $9.5 million next year in federal dollars.***
>
> *"That's one of the major drivers in our deficit," Swan said. HFCC distributed $110 million in financial aid last school year.*
>
> *Tuesday's board meeting coincidentally fell on the winter semesters NA day — the day faculty mark if a student has never attended. Students marked NA are cut off from receiving any more of their financial aid from HFCC. The college still has to repay the tuition and fees part of any Pell grant that person received, but at least is not on the hook for the rest of the money.*
>
> *HFCC Federation of Teachers 1650 President John McDonald said his union, in the last four years, has taken both pay cuts and increased insurance contributions that equate to about a 10 percent salary reduction for most employees. They also agreed to delay filling 19 positions, which saved the college about $1 million.*
>
> *Some Pell runners, however, have figured out the system and will attend for a few days early in the semester and then stop coming once the checks are sent. Students can get Pell grants based on financial need, possibly receiving up to $5,500 a semester to cover tuition, fees and living expenses. But if students do not complete their classes that semester, HFCC must return all the money to the federal government. The college can go after the so-called "Pell runners" to have the funds repaid, but often with little success, College President Gail Mee said after the board meeting." (*Hetrick)

Summary:

There is a vibrant underground economy of tens of thousands of websites that offer homework, exams and even online participation for a fee. Additionally, thousands of fraud rings using straw students to apply for and receive grant monies has cost billions of dollars in fraud and reduced the pool of aid for all students. This fraud affects an institutions budget by forcing tuition increases, cost savings programs and job losses.

The Department of Education reacted to these trends by mandating new student ID verification regulations in the 2008 education act (Part 602, Subpart B, 602.17 g). This was to put a process in place to verify the registered student is the same person who is accessing and completing the online course and materials. In spite of sending out Dear Colleague letters increasing fraud instances and Congressional oversight led the OIG to conduct audits to determine compliance to the Education Act by colleges and universities. Fast forward to today's environment.

Present day environment:

Compliance by institutions to the 2008 education act and lack of response to Dear Colleague letters to put student ID verification and attendance measurement processes in place has been poor or some say non-existent. Encouragement to put these processes in place was also detailed in the U.S. Department of Education Office of

Inspector General report January 2013 titled, "FY 2013 Management Challenges". This report stated more oversight was needed and Distance Education was one of 4 major management challenges because student ID verification was difficult, resulting in fraud and attendance reimbursement miscalculations.

To determine how widespread the lack of compliance was the Office of Inspector General (OIG) within the Dept. of Education conducted audits in 2010 and 2011 including reviewing 8 schools representing a cross section of 2, 4 year colleges and universities. The audit revealed that $222M was given in financial aid to 42,000 online students, none of whom received an academic credit. They concluded that none of the eight schools properly determined and documented students' academic attendance in accordance with the requirements promulgated in 34 C.F.R. § 668.22(c)(3). In addition, none of the eight schools used procedures that effectively verified students' identities as part of the enrollment process.

All eight schools reviewed required distance education students to have secure logins and passcodes. However, none of the eight schools had a specific process to verify student identity as part of the enrollment process. By themselves, logins and passcodes do not confirm the student's identity.

OIG audit results prompt new regulations:

The results of the audits and increasing fraud concerns prompted new stricter rules on student ID verification along with other rules that are now aligned with institutions continuing to receive Title IV funds. If colleges and universities don't comply with stricter student ID verification technology beyond PINs and passwords, and the other 5 rules (as detailed in their Final Audit Report February 21st 2014 that required action by the Department within 30 days) continued access to Title IV funds may be in jeopardy (Hetrick).

Pins and passwords are not enough:

The OIG Final report has stated that use of PINs and passwords are not enough to reduce fraud with Title IV funds. They are demanding better identity verification methods to be used.

> *"The reliability of logins and passcodes depends on the processes that schools use to verify identity before issuing the passcodes and on students' care in safekeeping such credentials. A secure login and passcode ensure only that someone logging in to a course is using the same login and passcode assigned to the person who enrolled. A secure login and passcode do not ensure that the person is enrolling under a valid name and intends to obtain an education. The regulations should be clarified and strengthened so that schools are required to use current best practices in identity verification methods to better mitigate the risk of student identity fraud".*

As the Final Report states, the reliability of logins and passcodes depends on the processes that schools use to verify identity before issuing the logins and passcodes and on students' care in safekeeping such credentials. As a result, logins and passcodes cannot detect individuals logging on with multiple identities or straw students involved with fraud rings. Additional requirements are needed to ensure that schools verify a student's identity as part of the enrollment process. Requiring the student to provide proof of name, high school diploma, educational transcripts or college admission test scores, would help corroborate identity, and ensure the student intends to obtain an education.

Data collection:

In addition, for an entity to run and control its operations, it must have relevant, reliable and timely communications. Information is needed throughout the agency to achieve all of its objectives. Program managers need both operational and financial data to determine whether they are meeting their agencies' strategic annual performance plans and meeting their goals for accountability for effective and efficient use of resources. In addition

to internal communications, management should ensure there are adequate means of communicating with, and obtaining information from external stakeholders that might have a significant impact on the agency achieving its goals. Moreover, effective information technology management is critical to achieving useful, reliable, and continuous recording and communication of information. (US Department of Education)

The six new rules:

The Office of Inspector General detailed 6 new rules to the Dept. of Education in their report ED-OIG/A07L001. They were all accepted by the Dept. of Education. Of these new rules, three focus on institutions that deliver distance education to have:

1. New stricter student ID verification measures,
2. Academic attendance audits and
3. More and longer period data collection to mitigate risks associated with fraud.

There is no such thing as close to compliance or 80% compliant, as some institutions may try to suggest. Failure to comply means risking continued participation with Title IV funds. The report details the following processes must be place to fully comply with Title IV requirements.

Excerpted in its entirety from the Final Report is the following:

A school offering distance education must do the following to comply with Title IV requirements:

- require selected applicants to verify their identity as part of the student aid verification process (Dear Colleague Letter GEN-12-11, July 17, 2012);

- establish a process, acceptable to its accrediting agency, to verify that the person who registers in a distance education course or program is the same person who participates in and completes the course or program and receives the academic credit (34 C.F.R. § 602.17(g));

- determine the withdrawal date for a student who withdraws from the school (34 C.F.R. § 668.22(b) and (c));

- ensure that, when determining a withdrawal date or whether a student has begun attendance, it adheres to the definition of academic attendance and attendance at an academically related activity (34 C.F.R. § 668.22(l)(7), effective July 1, 2011; 34 C.F.R. § 668.21);

- resolve Institutional Student Information Record (ISIR) codes flagging students with unusual enrollment histories in accordance with Dear Colleague Letter GEN-13-09 (March 8, 2013); and

- develop and follow procedures to evaluate the validity of a student's high school completion if the school or the Secretary has reason to believe that the high school diploma is not valid or was not obtained from an entity that provides secondary education (34 C.F.R. § 668.16(p), effective July 1, 2011).

- In addition, the Department specified by regulation that evidence of a student logging in to an online class is not sufficient evidence by itself to demonstrate academic attendance by the student (34 C.F.R. § 668.22(l)(7)(i)(B)(3), effective July 1, 2011; 75 Federal Register 66898-66899, October 29, 2010).

New oversight:

"Since 2005, the Inspector General has testified before Congress five times on the susceptibility to fraud and abuse of Title IV programs delivered to students enrolled in programs of study offered through distance education". Since FY 2010 when the Pell Gant improper payments of $1.0 billion exceeded the OMB FY 2010 high-priority program threshold of $750 million, the Department has to establish semiannual or more frequent measurements for reducing improper payments in the program and prepare an Accountable Official's Annual Report (US Department of Education).

In other words, too much money is at risk. Since the Department of Education is now accountable to Congress, it falls to the individual institutions to be accountable for identity fraud. But who has oversight for this?

Other important information:

The Final Audit Report talks about whether the state and accreditation agencies have been providing the necessary oversight to manage the unique compliance challenges detailed below:

"We identified the following requirements that present unique compliance challenges for schools offering distance education:

- *verifying a student's identity;*
- *determining student attendance at an academically related activity; and*
- *maintaining sufficient evidence of a student's academic attendance.*

√ They stated categorically that oversight has not been adequate.

> *"Collectively, the oversight provided by the Department, accrediting agencies, and States has not been adequate to mitigate the risk of schools not complying with the requirements that are unique to the distance education environment".*

√ The report spoke to the issue whether accreditation agencies or individual states should have the responsibility to monitor a schools compliance in these areas. They stated that only the Department of Education has this responsibility.

"Accrediting agencies and States have minimal or nonexistent responsibility to monitor a school's compliance with the Title IV requirements. An accrediting agency's role is to monitor a school's academic quality, while a State's role is to authorize and license schools. Therefore, The Department is responsible for promulgating Title IV regulations, authorizing schools to participate in the Title IV programs, and monitoring a school's compliance with the Title IV requirements." (US Department of Education)

The report discussed the role of accrediting agencies in re-evaluating that schools have processes in place to ensure that the student who registers in a distance education course or program is the same person who participates in and completes the course or program and receives the academic credit.

However, the primary purpose of accrediting agencies is to ensure the quality of education or training offered by accredited schools, not to evaluate identity verification processes or assess whether a school's system of internal control over administration of Title IV programs is operating as intended. Additionally the accrediting agency reaccredits schools on cycles that ranged from 3 to 10 years and cannot be effective. (US Department of Education)

√ So to put their own process in place, the Department will ensure the following is adhered to:

> *"Schools participating in the Title IV programs are required to have annual compliance audits conducted by an independent public Final Audit Report ED-accountant. The purpose of the annual compliance audit is to provide the Department with reasonable assurance that the school is complying with the Title IV requirements. Part of the audit process is to ensure that the school is complying with Title IV requirements by testing the school's processes.* ***Therefore, the independent public accountant already is required to verify that the school has implemented Title IV-related processes and confirm that those procedures are operating as intended".***

√ ***Fundamentally this means that once yearly if the independent auditor does not feel the institution is in compliance, Title IV funds can be cut off and investigations could begin by the OIG to determine what tuition funds may need to be paid back and what processes need to be put in place to meet compliance.***

Academic Integrity, Student ID verification and Financial aid fraud:

It may be a good time to discuss the differences between academic integrity, student ID verification and financial aid fraud. While definitions abound, we have come up with what we hope is some workable ones.

Academic integrity/dishonesty is an attempt to misrepresent work, effort, materials as your own yet, others have contributed in whole or in part make the effort no longer unique to you. Integrity is generally dealt with through the schools code of conduct, plagiarism checking software, browser lock downs and physical or online proctoring. Proctoring can verify that a person who is taking the exam can present a government issued ID or similar form of identification with the correct name and whether the person is the correct sex. We do not know absolutely if that ID presented is from the real person stipulated. If the person is asked to answer security questions or use their phone as a verification credential, we still do not know if they are the real person. However, when we add dimensions of time, location and history to the identification process, we establish best practices by providing the highest levels of confidence the person is who they say they are. Because proctoring lacks these extra dimensions when determining identity, it is only useful in reducing obvious cheating for a single exam/activity. Because of the set up and cost constraints proctoring is not useful for all other gradable activities for a student.

Student ID verification: Verification of identity is in person or remote (meaning from a computer or portable device). Identification is usually accomplished by the use of credentials including:

- Something you HAVE – a physical document/transcript/card,
- Something you KNOW – information only the real person should know, and
- Something you ARE – always a biometric whether physical or behavioral.

Note, these credentials are used/combined differently depending if the identification is in person or remote. Authentication of identity is always a biometric**. Verification and authentication are used by most interchangeably but they are different. Authentication is not a single point in time but a continuous process. When we add in the dimensions of time, location, and history to a biometric we achieve best practices and the highest confidence levels the person is who they say they are.**

Financial aid fraud is when a person applies for financial aid without an intent to use it to advance their education. Persons can use other person's identity with or without their permission, once or multiple times to apply for and maintain a presence long enough to receive financial aid with the intent to defraud.

Meeting compliance using best practices:

Best practices include the following:

1. A process of student ID verification that can establish if the registered student is the same student taking the classes and doing the work. Pins and passwords are not enough, proctoring is for academic integrity only and is not a solution for ongoing student ID verification.
2. Begin student ID verification processes as early on as possible with first contact with the student and then throughput the course at any/every gradable event not just exams. In an 8 week session for example, if you only assess a student at the final exam, who has been doing all the tests, quizzes and participation for the last 7 weeks?
3. Combine verification of identity before you provide the student their access pin/password to their learning management system and then add time, location, and history to a biometric to establish the person is who they say they are before they can access any gradable event.
4. Manage the collection of student credentials and look for fraud patterns using IP addresses, Death master files and other information OR use a third party to collect and review this work.
5. Choose a system that integrates with the LMS system and gradebook.
6. Choose a system that is flexible enough to also be used as a single sign on for any transaction between the student and the institution.
7. Choose a system that is flexible enough to be used as an identity authentication to reduce academic dishonesty AND financial aid fraud due to identity fraud.
8. Choose a system that can provide both real time and historical reporting that has an audit trail report, tracking and suspicious activity tool.

2.0 Introducing Biometric Signature ID:

Biometric Signature ID (BSI) is an award winning company specializing in the field of Multi-Factor Authentication for identity and access management solutions.

BSI has created BioSig-ID™, a software only biometric with two issued patents, to secure data and devices without the need for any additional hardware. Using only a mouse, finger or stylus, gesture biometrics of speed, direction, length, height, width, angle are captured and stored in an enrollment profile as the user draws and creates their unique passcode. Upon subsequent logins the software compares the passcode entered to the unique passcode the user created, providing instant authentication. However unlike a regular typed in password, only a user who has been successfully authenticated can gain access to their virtual account, gradable event, portable device, workstation or mobile app. The data is encrypted at rest and in transit.

BioSig-ID was awarded “New Product Innovation of the Year in North America”, selected as Top 20 Most Promising Ed Tech Companies out of 500 companies by the prestigious CIO REVIEW (Oct 2014), was independent third party tested at 99.97% accuracy, reports a 98% user satisfaction rate and has nearly 4M uses from over 70 countries and all 50 states. The technology has been featured in 14 education and security publications in the previous 6 months, including Dean and Provost, eCampus News, Successful Registrar, Enrollment Management and Community College Week. In education, BSI has over 90 colleges and universities as clients.

BSI was chosen and funded by the White House (from 180 other companies) to participate with Microsoft, AT&T, CA, AAMVA and the Virginia DMV in a pilot to reduce online identity fraud. BSI is also a selected committee member with the North American Security Products Organization (NASPO) that has been selected by the federal government to develop the next official standards for identity proofing. This is a high power group consisting of government agencies, multiple governments and top leaders from US companies.

The software product - BioSig-ID™, does not require any hardware providing a cost effective solution that can be used on any PC, tablet or cellular device with Internet access. Compared to passwords, security questions or proctoring, BioSig-ID delivers a process that ensures compliance with current accreditation and education act regulations and the new Office of Inspector General (OIG) mandates for continued access to Title IV funds.

However there is good news for schools who are worried about maintaining Title IV funds.
BSI offers a compliance solution to the new mandates as detailed in the slide below.

Results of OIG Audits = 6 new regulations

- **4 regulations require stiffer:**

-student identity verification
-academic attendance audits
-more data collection to mitigate risks
-more frequent review of processes every year

- **1 regulation deals with state authorization**
- **1 regulation deals with costs of attendance**

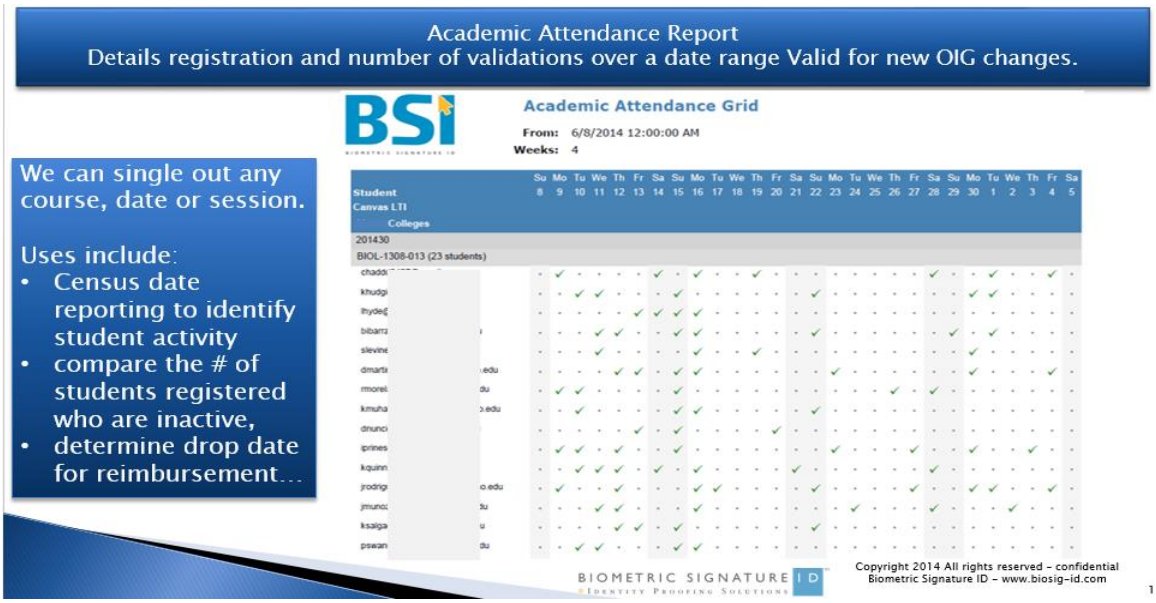
BSI has years of experience with all types of colleges and universities with nearly 4M uses and is an expert in the implementation and deployment of our student ID verification solution. We have students using BioSig-ID to verify their identity from 70 countries. Part of the value proposition is that unlike other biometrics no special hardware or software downloads is needed. BioSig-ID has been used to "gate" any gradable event inside all major LMS systems using adaptive release or adding it as a content item.

"Gating the front door" permits only the registered student with a pattern match access to the gradable event, thereby ensuring that only the correct student is doing the course work. Some clients have also done away with physical or online proctoring completely and replaced them with BioSig-ID to maintain academic integrity. When BioSig-ID is used we can compare the historical pattern of previous student authentications and when any gradable event/exam is attempted only the correct student gains access. Just by announcing the use of BioSig-ID, known cheaters have dropped out of courses that require identity authentication. The level of deterrent is similar to when gas stations did not require the entry of a zip code. This one additional step cause a drop in fraud by over 80%.

BioSig-ID's newest security feature is real time event handling. Now we establish a set of rules or events that when they occur will send an alert in real time to the administrator. These will alert the institution of suspected fraud activities. Examples include time, location (IP) and geography events that are not consistent or normal. These alerts are pushed to the clients and appropriate follow up is completed by BSI and the client.

Our costs for the entire year with unlimited authentications regardless of number of courses is 50%- 80% less than ONE session of physical or online proctoring. Surveyed students actually preferred BioSig-ID 96% in favor versus physical proctoring and in several evaluations no difference in grades was noted. Proctoring only attempts to catch cheaters on a single test, BioSig-ID does the entire course.

The software comes with a robust audit trail providing an acute forensic tool to help identify online fraud leading to academic dishonesty and financial aid fraud. An example of the Academic Attendance report is shown below. BioSig-ID provides a comprehensive set of rich data that can establish fraud manifested in academic or financial aid fraud. This data is different than what is offered from third parties or what most schools may do internally. It has to be.



What is currently used is not enough. If it was we would not see the fraud we see. **The most logical solution is to combine our real event handler and historical data with the school's data for the best predictive outcomes**.

Compared to other biometrics like fingerprint or iris scanning BioSig-ID gesture biometrics do not require any special readers or maintenance. Our reader is in the cloud making access universal. Keystroke biometrics fall into the same class of dynamic biometrics as gestures. However due to lack of specificity, independent tests by the same lab that tested BioSig-ID found keystroke analysis was 27x less accurate then BioSig-ID. Their results did not meet the minimum National Institute Standards and Technology (NIST) guidelines. BioSig-ID by comparison exceeded these guidelines by a 3 fold factor making the technology far more accurate and superior. This was one of the reasons the White House NSTIC project chose BioSig-ID technology over 180 other companies/consortia.

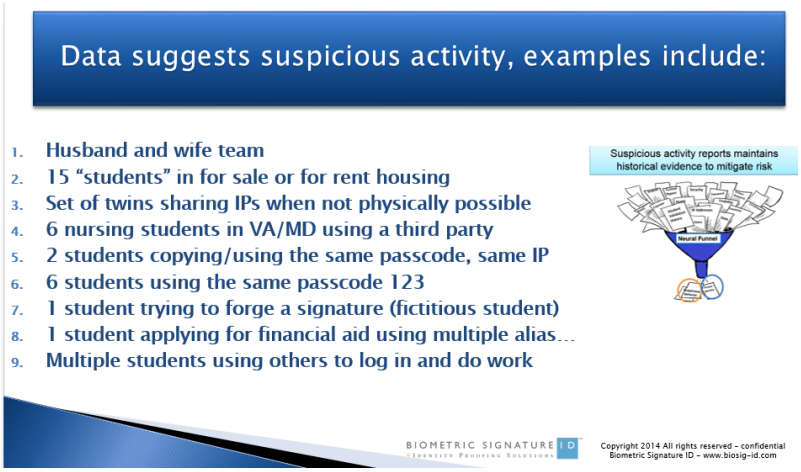
The User Experience

In surveys to first time users, 98% reported they had a positive experience with BioSig-ID. This group was widely different in terms of age, demographics, location and race. Of interesting note is that 45% of first time users surveyed reported that BioSig-ID had an entertaining quality. We have seen that users will spend a lot of time in the system attempting to play/game the system. We have reported that one user validated their identity a total of 81X at a single setting and that another user spent nearly 3 continuous hours validating their passcode. These are the current records!

Based on independent, third-party testing performed by the Tolly Group and from user surveys, BioSig-ID™ has the following proven results:

- 99.97% Protection against imposters
- 100% of users surveyed were able to enroll with BioSig-ID™
- 98% of users found BioSig-ID™ easy to use
- 96% of users believed it impossible to break into another's passcode

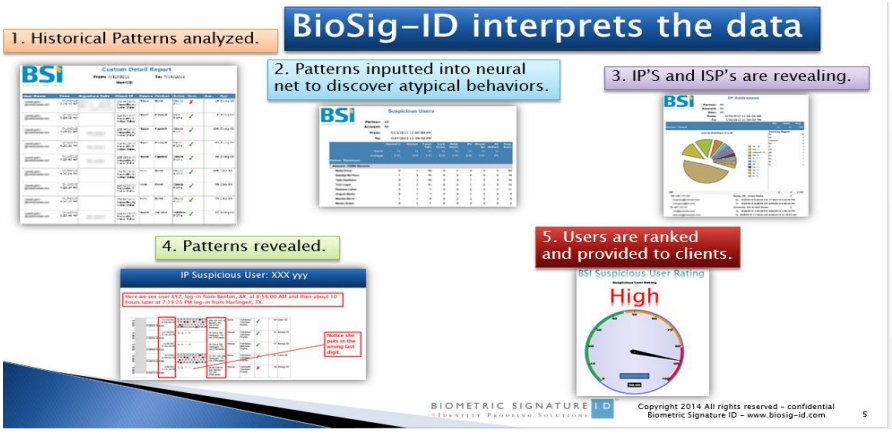
In a recent analysis of over 710,469 validations in our system, 3,778 required assistance from the help desk or less than 1%. Passcode resets by unique users were done at 2.5%. These values are extra-ordinary low since normal help desk calls and resets are usually close to 50% versus our 1%. We believe this is due to our ease of use.



An example of the types of suspicious activity that has been identified as fraud using the BSI data mining technology is shown opposite.

BSI is working with a number of the largest institutions in higher education, financial services, online gaming and healthcare, providing identity authentication before users can access exams, bank accounts, corporate assets or personal health information. We have presence and expertise working with all types of courses, students, locations and institutions.

Report tools



BioSig-ID provides a standard and premium suite of reports.
Using our advanced neural net predictive technology we are able to use data mining to capture suspicious activity. Using time, location (including IP's) and history we can uncover identity fraud leading to academic dishonesty and financial aid fraud.

How does BioSig-ID™ work?

BioSig-ID™ is a patented, software-only biometric solution that provides the strongest method of identity authentication on the market today. The software measures the unique way a user moves their mouse, finger or stylus when they log in with a passcode created with BioSig-ID™. Biometric gestures such as the length, speed, direction, angle and height of each stroke are collected by the software to create the user's unique biometric profile. In seconds and after drawing only 4 characters, BioSig-ID™ software establishes whether the student who registered for the course is the same person accessing course materials and receiving credit.

Only a user who has successfully authenticated themselves against a previously created enrollment profile can access coursework, online discussions and all gradable events including exams. The software comes complete with a robust audit trail that captures all the activity surrounding the authentication event, providing an acute forensic tool to help fight academic and financial aid fraud.

BioSig-ID™ and Learning Management System (LMS) Integration

BioSig-ID™ easily integrates with your school's LMS (via a plugin or LTI) allowing faculty and staff to effortlessly access the current and historic activity of any BioSig-ID™ user. Ideal for both distance learning and traditional institutions, BioSig-ID™ can be placed as a gate when a student:

- Registers for school or financial aid
- Registers for a course
- Signs in for interactive discussions
- Signs in for actual coursework
- Signs in for a gradable event/exam

A leading cause of compliance audits and judgments, lack of student identity authentication represents a monumental risk to higher education institutions. BioSig-ID™ reduces this risk by providing the industry's most complete solution for student ID authentication.

Let us show you how to save money, stop imposters, ensure compliance and reduce your risks of reimbursements.

Call us today at 877-700-1611 or e-mail us info@biosig-id.com to schedule a no obligation web demo.

References

Cumming, Chris. "Worrisome Spike in Student Loan Write-Offs." *American Banker* (2014).

Dante, Jonathan Barkat/Ed. "The Shadow Scholar." *The Chronicle of Higher Education* 2010, Chronicle Review November 12, 2010 ed.

Delisle, Jason. *CBO Releases 2013 Pell Grant Funding Target*. 13 March 2012. 1 January 2015. <http://edmoney.newamerica.net/blogposts/2012/cbo_releases_2013_pell_grant_funding_target-65244>.

Hetrick, Katie. "Henry Ford Community College (Michigan) raising tuition, dealing with grant theft." *The News Herald* 5 February 2013. Web. <http://www.thenewsherald.com/articles/2013/02/05/news/doc5102d57a0d780419546356.txt?viewmode=fullstory>.

Joanne, Jacobs. "Financial aid cheats target online programs." *The Hechinger Report- Community College Spotlight* October 2011.

Mitchell, Josh. "Student Aid Scams Targeted by Schools." *Wall Street Journal Online* (2013). <http://online.wsj.com/news/articles/SB10001424127887323300004578557393479395544>.

Office of Inspector General. "FY 2013 Management Challenges." 2013.

Testimony of Inspector General Kathleen S. Tighe. Tighe U.S. Department of Education Office of Inspector General before the Subcommittee on Labor, Health and Human Services, Education, and Related Agencies Committee on Appropriations. 19 March 2012. Document.

United States Attorney District of Arizona. *65 INDIVIDUALS CHARGED IN FEDERAL FINANCIAL AID FRAUD RESULTING IN THE LOSS OF OVER $530,000*. 24 June 2009. Web. 1 January 2015. <http://www.riosalado.edu/financial_aid/documents/fraud-pr.pdf>.

US Department of Education. "Title IV of the Higher Education Act Programs: Additional Safeguards Are Needed to Help Mitigate the Risks That Are Unique to the Distance Education Environment “Final Audit Report”." 2014.