BIOMETRIC SIGNATURE ID™
* IDENTITY PROOFING SOLUTIONS

Online Student ID Authentication

Reducing Academic Integrity Issues Using Real Time Event Notifications

Jeff Maynard, B.Sc. – CEO and Founder, Biometric Signature ID

BIOMETRIC SIGNATURE ID™
* IDENTITY PROOFING SOLUTIONS

Case Study

"We have worked with BioSig-ID to provide added security to courses. The staff at BioSig-ID have helped us to integrate the software into courses with very little training or support needed for instructors or students. We have seen no increase in help desk or technical support issues resulting from the use of BioSig-ID and the regular alerts and reports have helped us identify suspicious activity that we might not have caught before."

Director of Student Services

Background

Note: This is a use case report from a Biometric Signature ID (BSI) client who chooses to remain anonymous so persons who commit fraud are not informed of client's new security. We will refer to our client as "*BSI Client*". What follows is their report on how, used in combination, BioSig-ID's Real Time Event Notifications (RTEN) and Suspicious Activity Reports (SAR), and features within their Learning Management System (LMS), enabled proactive filtered alerts to identify academic integrity patterns.

BSI Client is a consortium of 13 colleges, serving around 12,000 students per semester. It is an extension of, and a service to, each of the home colleges it serves. BSI Client offers students another learning option for complementing their on-campus experience. By offering courses through BSI Client, the home colleges are able to offer their students courses and programs that they may not be able to offer individually.

Quote from BSI Client:

"As a school we understood our online students were tempted to share logins, use third parties for hire, and/or surrogates from foreign countries. As a school we researched known vendors and available new technologies for both integrity and new Title IV regulations. We began using Biometric Signature-ID (BSI) as a Learning Technology Integration (LTI) in ten courses the fall of 2014. Biometric Signature ID (BSI) was chosen for the following reasons:"

Review of Available Technology for Test Security - **Comparing Solutions**

Attributes	Live Video Proctor	Passive Video Proctor	Biometrics
Assure student's identity	Y	Y	Y
No extra cost to student	N	Y	Y
Predictable cost to CCCO	Y	Y	Y
No extra technology	N	N	Y
Runs on all networks	N	Y*	Y
Works on pc, mobile devices	N	N	Y
Available 24 / 7	Y	Y	Y
Available w/o appointment	N	Y	Y
No instructor responsibility	Y	N	Y

Client Responses on BSI Project

Technical Implementation

"BioSig-ID (BSI) can be easily integrated into our LMS using Learning Tool Interoperability (LTI) links. Gating assignments in BS is done via release conditions within the LMS. Placing BSI LTI links within the course creates associated grade book entries that can then be used as a release condition trigger on any item that supports release conditions, such as quizzes, drop boxes, or content items. The end user must then open the gate to their assignment by completing BSI authentication using the LTI link. The effectiveness of this method of gating depends on the length of time the assignment is available and shorter assignment availabilities are advised for maximum effectiveness."

System Administrator

General Information

- BSI Client gated 10 courses with multiple sections fall and spring, 2,900 students total
- Helpdesk impact was very minimal, maybe 6-10 calls a semester

Challenge

BSI provided us with a historical report called a Suspicious Activity Report (SAR). This report identifies the user experience and then analyzes up to 20 metrics from our student body using time, location, activity and history. These metrics define a sub set of students whose activities are ranked as being highest in suspicious activities. Linking various reports together BSI is able to take a closer analysis of suspicious activities to identify ultimately whether the registered student is the same student doing the course work. The SAR report forms a baseline of activities that may be unique to our particular school and students.

"What our administrators asked for was to have a proactive method to be able to act on suspicious activities. The new software version from BSI introduced in January 2015, implemented the Real Time Event Notification (RTEN) which gave us the detection we needed to investigate in a timely manner."

Dean of Academic Technology

The RTEN alerts are a combination of SAR - ID authentication activity data, which are weighted based on the combination of activities. These recognized pattern activities activate predefined RTEN event alerts. The alerts have been weighted to send via email or SMS as a low, medium or high status.

The goal of revealing integrity issues had to meet certain factors:

- Make online assessments more secure
- Adopt minimally intrusive methods for students
- Don't add work to faculty
- Keep costs down

Results

- Of the 78 students identified within 125 RTENs received from BSI (47 were duplicate students performing the same activity), 46 students had documented cases of suspicious activity in various courses during the spring term. (59% identification rate).

- The BioSig-ID system can shut down access to the assessment per client's instructions based on certain trigger events. Clients currently prefer to let students proceed, while the school gathers more information before a next action decision.

- Events can be triggered when a professional test taker tries to access the assessment. Trigger events like password resets at time of exam, different/foreign IP's, different devices etc., were captured. The surrogate may have aborted or never gained access to the assessment.

- The value of collecting all this activity over time cannot be overstated.

- 19 Suspicious Activities Reports (SARS) were directly attributed to the RTEN's.

- 27 SAR's were leads found in the first 19 investigations.

The combinations of BSI detection tools and LMS IP data tracking and reporting functions made this possible. The "BSI Client" determined that a student has violated student policy if they have given their login to another person who attempted or completed access. It was possible to both show that in all 46 cases and also document the IP address of test takers who were not the student in many cases.

After receiving a BioSig-ID RTEN, this was the reviewprocess:

Step 1 - Pull a BioSig-ID Custom Detail Report on the students test login history for 60 days

- Look for pattern of login failures, clues:
- IP Address timing issues
- Changing IP address
- Test time coincidence with login failure?
- Or reach out to student to assist with login issues

Step 2 - Send to Student Services for Review and Action

- Warning letter
- Further action if needed

Summary

"Overall BSI has been an easy vendor to work with. They are eager to find ways to help us be successful. The SAR baseline report is historical, which indicates the potential for suspicious activities. What our administrators asked for was a proactive method to act on those suspicious activities. The new version in January implemented the Real Time Event Notification which gave us the detection we needed to investigate in a timely manner."

Dean of Academic Technology

The combination of BSI's Real Time Event Notification (RTEN) and BioSig-ID standard report tools, using LMS IP Tracking tool, and the Quiz Log with IP addresses, has made it possible to do appropriate investigations of suspicious student activities.

The RTEN operates on a set of parameters around the student's time/location, password resets, and successful logins and login failures. These settings are discussed at the beginning of the term and sometimes adjusted to the outcomes found. The RTEN's are sent via email to a number of administrators, and in our case, one person had the responsibility to review and determine whether to further investigate. By using the BSI custom reporting tool, the investigator can pull up a report going back as far as necessary in the matter of a minute.

The report shows the pattern of success and failure, date and time, device used, course, IP address and location. There are unique patterns often associated with third-party test takers using the student's password to enter the test. In our instance, BSI was used only on assessments.

Once patterns are seen, such as IP timing issues with the student and the test taker in different locations at the same time, the student is deemed in violation of student policy on sharing passwords. Sometimes, the BSI report is supplemented with data from the IP tracking tool to get a fuller picture of what the student is doing at other times, when not taking a test. The LMS quiz tool also has a great feature that allows the instructor or administrator to see the IP address of every part of the quiz as it is saved.

Another useful tool is the LMS Reporting Tool, which allows the administrator to search for the student user and/or test takers session to see how long those sessions lasted. This can be helpful in determining IP timing conflicts. Once IP's have been identified through the BSI custom reporting process, and they seem to be ones that are used by test takers, these IP ranges can be run back through the LMS Reporting Tool to further uncover possible third-party test takers. We've had success with this strategy.

In conclusion, as additional RTEN predictive pattern recognition alerts are created, and we fine-tune our skills with the tools we have. We are confident that our courses are secure, and that grading for all students is being done fairly, not influenced by professional test takers.

June 2015

Editor notes:

The focus of this client was on academic integrity, and to ensure grading was done fairly and not influenced by professional test takers. BSI is also analyzing students who are committing financial aid fraud. Using our report tools, like our academic activity /attendance report to evaluate students who register for courses but do not complete any "academic activity" (i.e. using BioSig-ID authentications), we can establish non-active students, and potential Pell runners. BSI's forensic report tools employing time, location, activity and history have helped to identify students who have no intent in going to school and are lasting in class just long enough to pick up their grant monies.

The increase of large fraud rings and ease of obtaining FSA has made this a vibrant underground where $B's of dollars are being diverted. It is estimated that up to 4% of financial aid disbursements are improper payments and fraud. The recent Office of Inspector General and Dept. of Education Final Audit report call for stricter student ID verification methods beyond pins and passwords, better academic activity measurements and more data collection to uncover patterns of FSA fraud. Compliance to these standards are now tied into continued access to Title IV funds. Proctoring is not compliant with these new regulations.

Many schools are already reimbursing millions of dollars yearly from students who receive grants and then walk away. Many students are also fictitious. BioSig-ID has become a new risk management solution that can help identify fraudulent students and reduce financial aid fraud. BioSig-ID combined with data from your institution ***can potentially save your school millions in reduced paybacks****. BioSig-ID gesture biometrics and forensic reports offer a timely and cost effective solution.*

For more information please read a copy of the White Paper - "Student ID Verification, What Institutions Need to Know"
http://biosig-id.com/images/docs/Student_ID_Verification_What_Institutions_Need_To_Know.pdf