

---

## **Identity Proofing for Online Student ID Verification: Report of Pilot with Houston Community College**

---

Prepared by:

**Stephen Levey, Ed.D.**  
Associate Vice Chancellor, Academic Instruction  
Houston Community College

**Jeff Maynard B.Sc.**  
CEO and Founder  
Biometric Signature ID

January 17, 2011





## Case Study

### “Identity proofing technology for student ID verification using signature gesture biometrics”

#### Abstract:

*Section 602.17 of the re-authorized Education Act of 2008 now requires an institution that offers distance education to have processes through which the institution establishes that the student who registers in a distance education course or program is the same student who participates in and completes the program and receives the academic credit. The Southern Association of Colleges and Schools, HCC’s accrediting agency, also makes the same recommendation.*

*To meet these new requirements/recommendations and test a solution that would allow more computer based exams at home while maintaining the highest integrity levels, Houston Community College contracted with Biometric Signature ID to run a proof of technology using their dynamic signature/gesture technology to authenticate student identity remotely.*

*Over a 2 month period (October 4-November 30, 2010) 140 students from multiple classes volunteered to authenticate their identity from their own computers using BioSig-ID and Click-ID software. Test subjects were asked to enroll, create a profile and authenticate their identity at various times during their course. Full audit trails were analyzed of all activity and an online survey was administered. The proof of technology was deemed very successful with 100% of participants able to enroll and validate. A substantial majority of the participants (87%) responded to the survey with 98% of participants reporting they had a positive experience with the software and 93% reported the enrollment was easy to extremely easy. Combined average time of enrollment in both BioSig-ID and Click-ID was 2 minutes and 56 seconds, while authentication averaged 26 seconds. Nearly 5,100 signature enrollment/authentications were completed by the participants in 69 days for an average of nearly 37 activities per participant. The use of signature/gesture software from Biometric Signature ID proved to be effective in authenticating student ID multiple times during the course. These results confirm earlier published results using BioSig-ID technology at University of Maryland University College and University of Texas Telecampus (9 campuses).*

*Based on the results of this technology pilot, we confirm that the BioSig-ID authentication software using just a mouse can be a useful and practical tool for remote identity proofing to authenticate student identity that requires little administration and no additional hardware.*



## Introduction

Many educational institutions are looking for a student identity verification solution to help manage growth and compliance issues with the Higher Education Opportunity Act of 2008 (HEOA) released in late 2009. Currently, HCC uses userid and password access to all online courses provided by its learning management system. Although that practice now meets current standards, the HEOA mentioned above and SACS policies indicate that higher educational institutions must continue to implement additional and improved methods to help ensure students participating in online courses, and taking online exams, are the same individuals enrolled in the classes.

As more courses are delivered online, college systems like Houston Community College (HCC) are also looking for alternatives to facility limiting on-site proctoring. A solution with the ability to offer student ID authentication for taking exams online and authentication for non-exam courses is desirable. The ideal solution(s) should also respect student privacy, be delivered at random, periodic points in the delivery of course content, be cost effective and offer the highest deterrent to academic cheating.

HCC selected Biometric Signature ID's (BSI) BioSig-ID as a promising identity proofing biometric technology for the pilot. The BioSig-ID software does not require any additional hardware or software downloads, can be used on any PC anywhere, anytime and does not collect personal identifying information. In comparison to more traditional verification measures like pins, passwords, tokens and knowledge based questions BioSig-ID's patented dynamic biometric technology cannot be borrowed or shared. In contrast to other more traditional biometrics like fingerprinting, BioSig-ID does not require hardware to be activated. Instead, BioSig-ID is software only and is activated using flash, a component used in all computers. BioSig-ID provides physical authentication of the user by measuring unique characteristics of the individual commonly referred as "something that you are". The user signs or draws their password in the software using just a mouse, stylus or touchpad. The software also incorporates "something that you know" making it a true multi-factor authentication system and ideally suited for remote authentication for students.



Academic integrity concerns are real amongst administration and faculty. Several recent studies described by McNabb and Olmstead within the University of Texas campuses found that:

- 76 faculty members with experience teaching both on-campus and online were surveyed. Forty-three percent indicated a belief that undergraduates cheated often or very often, and another 43% thought they cheated occasionally. Additionally, 68% believed graduate students cheated at least occasionally.
- About one-half of faculty members said they believed that the likelihood of a cheating in an online course was the same as in an on campus course. Nevertheless, 26% of faculty members thought that undergraduate students were more likely to cheat in an online course, and 13% believed the same about graduate students.

Looking at online courses versus campus courses, Olson and Hale surveyed 51 administrators at five campuses within the UT System in 2000, and 26 at the same campuses in 2006. Their survey explored attitudes toward online learning, including academic integrity. In both studies, more than 60% of administrators indicated they were more concerned about controlling cheating in online courses than they were for on campus courses.

An example of the level of serious cheating found by self report from the McCabe and Trevino (1993) research and 1997 update is found in Table 1.

TABLE 1  
Self-Admitted Cheating—Summary Statistics

Variable	1990–1991 (%)		1995–1996 (%)			
	1963 <sup>a</sup> (%)	1993 <sup>b</sup> (%)	No Code <sup>c</sup>	Code <sup>d</sup>	No Code <sup>e</sup>	Code <sup>f</sup>
Serious test cheating <sup>g</sup>	39	64	47	24	45	30
Serious cheating on written work <sup>h</sup>	65	66	56	32	58	42
All serious cheating	75	82	71	44	71	54

<sup>a</sup>*n* = 452. <sup>b</sup>*n* = 1,793. <sup>c</sup>*n* = 3,083. <sup>d</sup>*n* = 3,013. <sup>e</sup>*n* = 1,970. <sup>f</sup>*n* = 2,303. <sup>g</sup>Serious test cheating includes students who have engaged in copying on an exam—with or without another student’s knowledge—using crib notes on an exam, or helping someone else to cheat on a test or exam. <sup>h</sup>Serious cheating on written work includes students who have engaged in plagiarism, fabricated or falsified a bibliography, turned in work done by someone else, or copied a few sentences of material without footnoting them in a paper.



It is interesting to note the influence of a student code of conduct on cheating, which this research suggests reduces serious cheating from 71% to 54% in the latest reported analysis. Web sites like the following “teach” strategies of cheating, <http://exam-cheat.uv.ro/cheat.html>. Little research has been done on cheating in online courses. In research reported by Stuber-McEwen, et al, results suggest that cheating in online courses is not as pervasive as some believe, “when there is relative anonymity and a separation between instructor and student, these concerns seem to increase”. Thus, the need for colleges and universities to search for ways to increase online students’ connectedness to the online community cannot be overstated. They believed however, that as online learning becomes more accepted as a means to an educational end and available to more people, “it is likely that the prevalence of academic dishonesty will increase”.

### **Legislative Requirement to Authenticate Distance Learners**

The Higher Education Opportunity Act of 2008 (HEOA) requires accreditors to ensure that institutions have processes in place to assure that a person who registers in online courses also does the coursework. The Department of Education requires accreditors to make certain that institutions verify students’ identities through (1) secure logins and passwords, (2) proctored tests, or (3) identification technologies and practices as they become widely accepted. SACS, in its Distance and Correspondence Education Policy Statement, makes the same requirements.

The legislation is aimed at curbing academic dishonesty in online courses through misrepresentation. This pilot was an effort to gather information about HCCs students’ acceptance of the use of more stringent identification technologies beyond the traditional userid and password currently used by nearly all colleges and universities.

### **Biometric Technologies**

Authentication technologies use biometrics to confirm the identity of an individual through anatomical, physiological, or behavioral characteristics. Some biometric



solutions do not require any hardware. These are “dynamic biometrics” that are behavioral in nature. Dynamic biometrics offer the same identity authentication attributes as anatomical biometrics (such as fingerprints).

Unlike verification technologies, which confirm a user can demonstrate that they possess required information (such a password or the answers to personal questions), biometrics are difficult to duplicate and nearly impossible to share. Because authentication through biometrics can be applied to multiple course elements, assessments are not limited to tests as is the case with proctoring or monitoring (digital proctoring). Additionally, biometric systems have low implementation costs and staffing needs, unlike traditional and digital proctoring.

### **Houston Community College/Biometric Signature ID Pilot Project**

The primary goal of the pilot project was to gauge student acceptance of the use of Biometric Signature ID’s, BioSig-ID identity proofing technology for student authentication. Additionally, we wanted to compare our results from our college students to similar technology pilot projects completed at the University of Maryland University College (UMUC), the University of Texas System Telecampus, and independent testing completed by the Tolly Group, a group that assists technology vendors improve the credibility of their marketing collateral through third-party validation.

### **Houston Community College District**

HCC is one of the nation’s largest institutions of higher learning with more than 70,000 students each semester including more international students (8%) than any community college in the country.

The Houston Community College District was created under the governance of the Houston Independent School District, (HISD) as the result of a public referendum on May 18, 1971. In August of that year, more than 5,700 students enrolled in workforce education courses held at the Houston Technical Institute (housed in HISD’s San Jacinto



High School). In the following semester, academic transfer classes were added and taught at six HISD locations. Now, students can choose from the multiple campus locations of six colleges. Since its opening in 1971, more than 1.3 million students have improved their lives through education and training obtained from Houston Community College.

An open admission public institution, HCC awards associate degrees and certificates in academic studies and career and technology programs. HCC is committed to meeting the needs of its diverse communities, providing academic courses for transfer to four-year institutions, terminal degrees and certificates in more than 70 fields of work, continuing education and corporate training, lifelong learning and enrichment programs and the largest adult education program in Texas. In 2008, HCC was ranked 20th nationally in the Associate Degree Producer by Community College Week.

### **Biometric Signature ID (BSI)**

Biometric Signature ID's, BioSig-ID software gathers data on a student's mouse, stylus, or touchpad characteristics such as the speed, direction, height, length, width, and angle of the student's movements. These unique biometric characteristics represent the highest level of identity authentication and security. When a student enrolls in BioSig-ID, their biometric data creates a unique profile that is stored in a secure database. The student is authenticated when his or her actions match the unique profile on subsequent logins. To ease implementation and limit the need for student support, BSI provides two additional validation methods: Click-ID and Complex Security Questions.

Due to these multiple methods, a student only needs help desk assistance after failing to successfully be authenticated through one of the three methods. This helps limit help desk calls for password resets, while continuing to require the highest security login procedures.

BioSig-ID provides authentication of a user by measuring the individual's unique characteristics, commonly referred to as "something that you are." Click-ID and Complex Security Questions incorporate "something that you know." These multiple methods of authentication/verification make BioSig-ID software a true multi-factor authentication



system similar to those required for online banking. The BioSig-ID authentication system:

- is intuitive and simple to use;
- identifies students with a high accuracy;
- increases security within learning management and other IT systems;
- can authenticate tests, as well as other types of assessments such as written work and participation;
- does not require the purchase or installation of any hardware or software;
- can be used at login or for periodic, random challenges;
- may be integrated within the university website or portal, learning management system, student information system, or other similar technologies;
- can scale, to adapt to program growth;
- includes a process to easily distribute, revoke, renew, and replace credentials in the event of loss;
- only requires a student to create a profile one time during his or her relationship with the institution
- works across different channels of interaction, from desktops to smart phones; and,
- students' privacy is not threatened.

## **Methodology**

Students were recruited through e-mail canvassing and by faculty members, who were asked for permission to contact their students about participation. Involvement was voluntary and BSI offered token gift cards to ten participants chosen randomly. Students were asked to visit a customized website by the enrollment deadline. The website to which students were directed included written instructions and an instructional video.





Students were asked to spend about 30 minutes over the next 60 days creating a BioSig-ID profile and then to authenticate their identity with it six times. Specifically, they were asked to:

1. Watch a brief instructional video.
2. Enroll with BioSig-ID.
3. Enroll with Click-ID.
4. Select and answer Complex Security Questions (only if unable to be enrolled in BioSig-ID).
5. Be validated by BioSig-ID or Click-ID six times.
6. Complete a survey about the enrollment and validation process.

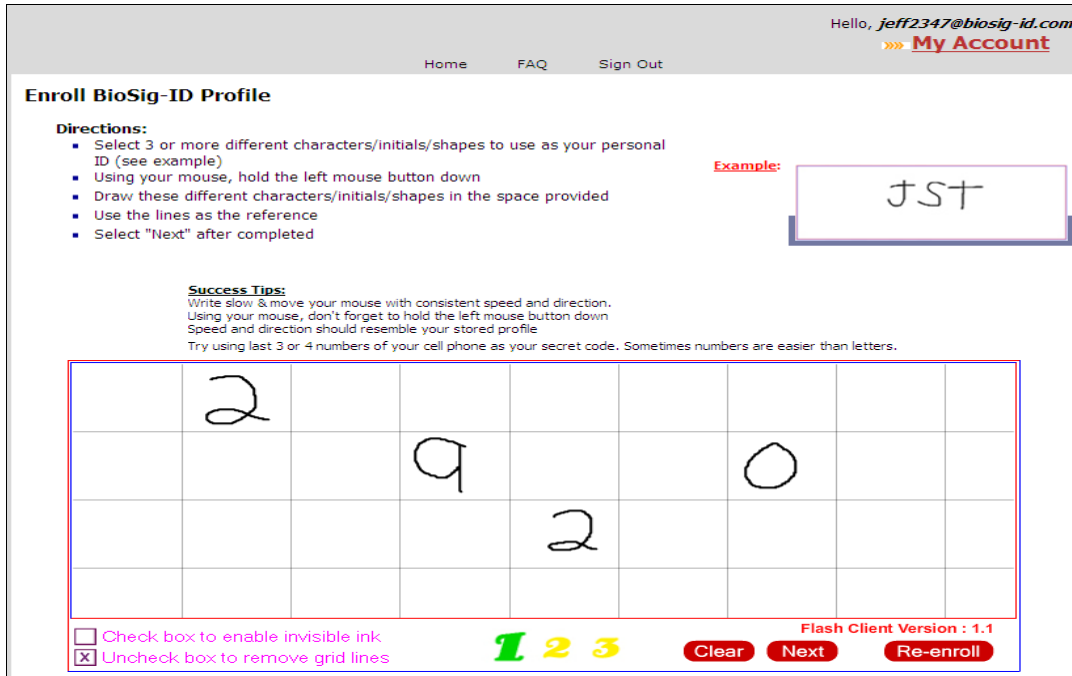
After the enrollment and validation deadline, email communications were limited to just the students who enrolled. Several reminders to complete six validations were sent to participants, as well as several email reminders about completing the survey. Additionally, students who finished the project received a Certificate of Completion by email.

Integration with the HCC learning management system was not a component of the pilot project. Therefore, access to HCC courses and services was not affected by a student's ability to be validated by the BioSig-ID system. Students accessed the authentication system on servers hosted by BSI, who also provided technical support.

## **BioSig-ID Enrollment**

Students started the process by registering and enrolling in the BioSig-ID system. Only an email address was required to register. After registration, a student was directed to a drawing screen with gridlines, as seen in Figure 1. Each student registered by drawing a “secret code” of his or her choice, made up of numbers and/or letters, within the grid. To complete his or her profile, a student had to repeat their secret code three times. When a student returned, he or she drew their secret code on a validation screen with the same gridlines. If the drawing matched the student’s enrollment profile, they were successfully validated.

**Figure 1. BioSig-ID Drawing Screen**



Hello, [jeff2347@biosig-id.com](#) [My Account](#)

[Home](#) [FAQ](#) [Sign Out](#)

### Enroll BioSig-ID Profile

**Directions:**

- Select 3 or more different characters/initials/shapes to use as your personal ID (see example)
- Using your mouse, hold the left mouse button down
- Draw these different characters/initials/shapes in the space provided
- Use the lines as the reference
- Select "Next" after completed

**Example:** JST

**Success Tips:**  
Write slow & move your mouse with consistent speed and direction.  
Using your mouse, don't forget to hold the left mouse button down  
Speed and direction should resemble your stored profile  
Try using last 3 or 4 numbers of your cell phone as your secret code. Sometimes numbers are easier than letters.

	2								
			9				0		
				2					

Check box to enable invisible ink  
 Uncheck box to remove grid lines

1 2 3

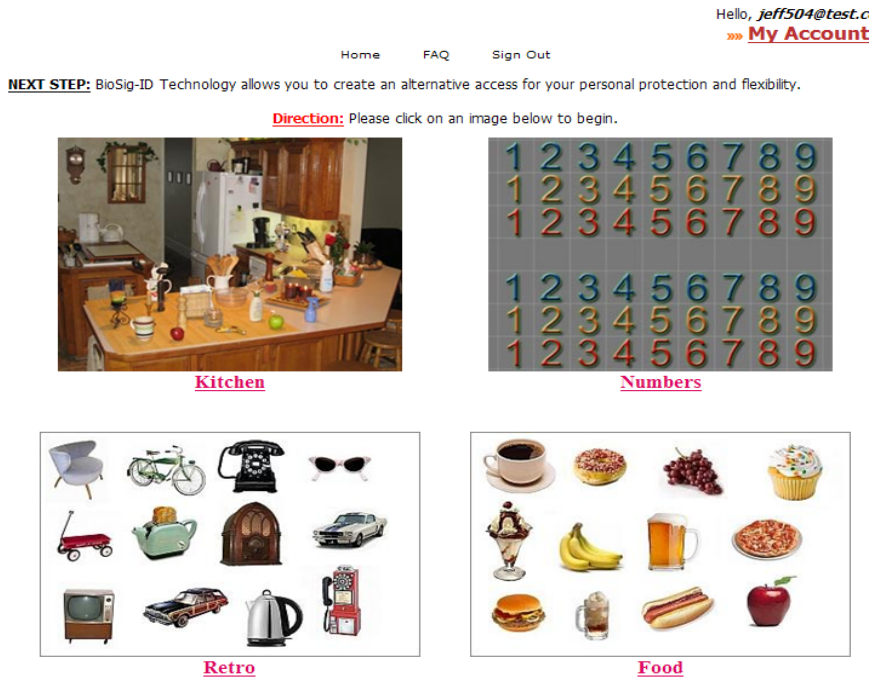
Flash Client Version : 1.1

If a student was unable to successfully create a BioSig-ID profile after five attempts, he or she was directed to Click-ID. The student's primary verification method would then be Click-ID.

## Click-ID

Regardless of whether or not a student successfully created a Bio-Sig profile, each also enrolled in a second, alternative verification method called "Click-ID." Each student chose an image from four options, as seen in Figure 2, and then selected three specific objects within in that image. To complete the profile, a student repeated their selections three times, in the same order.

**Figure 2. Click-ID Selection Screen**



If a student returned (if unable to be verified in BioSig-ID), he or she had to select the same image, and then the same items in the image in the same order. In addition, images were always presented differently on the verification screen (for example, compressed or elongated), for added security.

If Click-ID was a student's primary access method, successful verification gave them system access. On the other hand, if Click-ID was a student's secondary access method (they return to it because they are unable to be validated in BioSig-ID after three attempts), successful verification in Click-ID allowed the student to re-create his or her BioSig-ID profile.

## Complex Security Questions

Selected students (those who did not enroll in BioSig-ID) also answered two of 12 Complex Security Questions as a part of their registration in the BSI system. This allowed a student using Click-ID as his or her primary verification method, who could not validate himself or herself in Click-ID, to successfully answer personal questions to be given the opportunity to create new Click-ID profile.



## Results

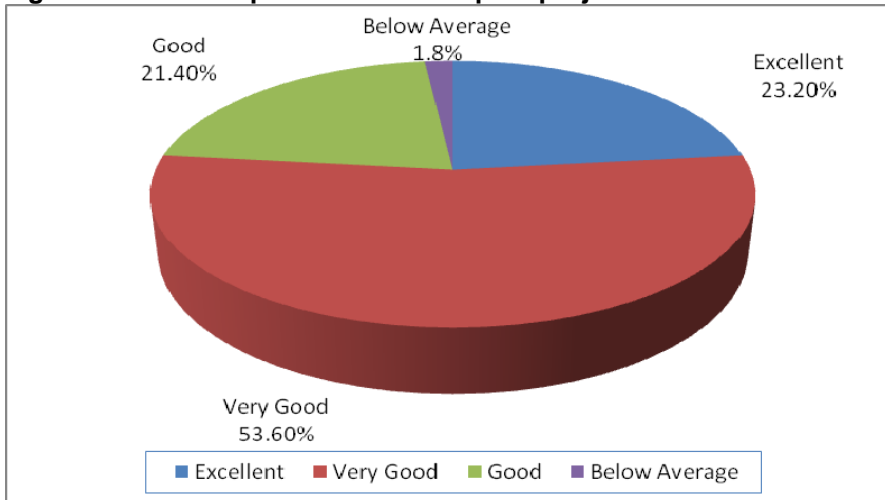
A total of 140 students completed the enrollment process:

- All students who attempted were able to enroll in the software.
- 98% of students who completed the pilot had positive feelings about their experience (rated “good,” “very good,” or “excellent.”)
- 131 of the 140 students completed the enrollment with BioSig-ID and Click-ID and 9 students enrolled in Click-ID Complex Security Questions.
- 75 students completed 1 – 5 validations while 65 students completed all 6 validations.
- 58 of 65 (89%) students completed the feedback survey.
- Combined average time of enrollment in both BioSig-ID and Click-ID was 2 minutes and 56 seconds, while authentication averaged 26 seconds.
- Three students contacted BSI for technical support. Two with a browser issue and one needed a password reset. In addition one student called for instruction clarification and two called for survey instructions but they did not complete the enrollment or validations.
- Participants completed 5,100 enrollments, validations, or re-enrollments in 69 days for an average of nearly 37 activities per participant.
- More than 70% of participants who enrolled confirmed they spent time experimenting with the system, purposely failing, testing the limits or completing additional validations.
- Participants gave very high marks for ease of use, simplicity and effectiveness in authenticating student identity.
- Closed loop technology (password reset) eliminated all help desk calls except the 3 as noted.

## Outcome

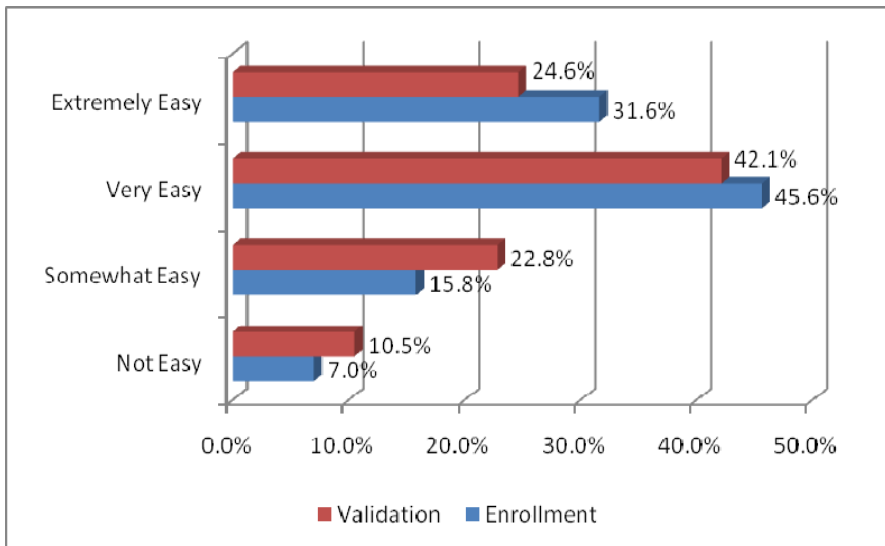
As can be seen in Figure 3, 98% of students who completed the pilot had positive feelings about their experience. Additionally, all the students (100%) who completed the survey indicated that the email and website instructions were easy to follow.

**Figure 3. Overall experience with the pilot project.**



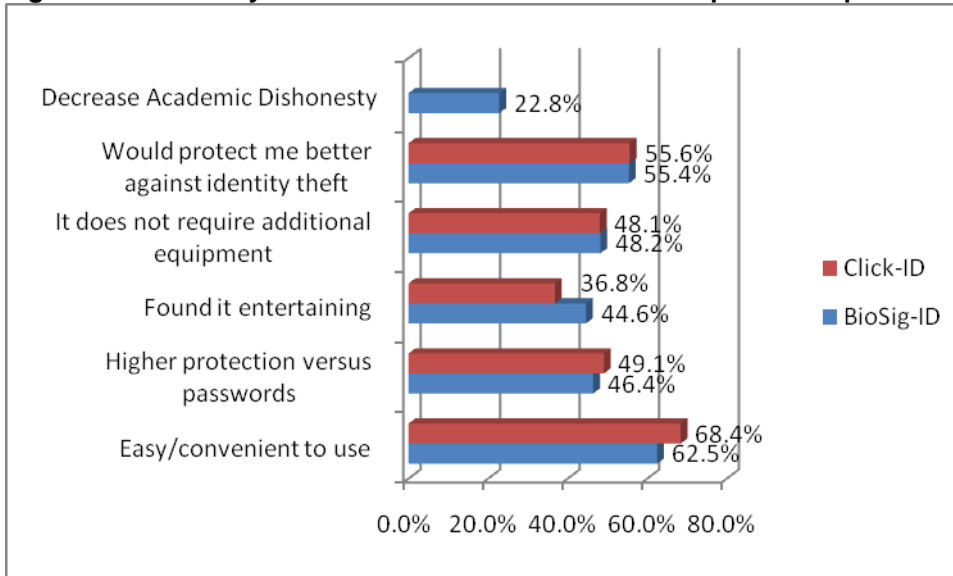
As illustrated in Figure 4, 93% of students who completed the pilot felt the enrollment process was easy and 90% said the same about the validation process.

**Figure 4. Feedback on ease of enrollment and validation from students who completed the pilot.**



All participants indicated the BSI’s system was convenient. This included 71% of the students surveyed, who said it was “extremely or very convenient.”

**Figure 5. Favorite system features of students who completed the pilot.**

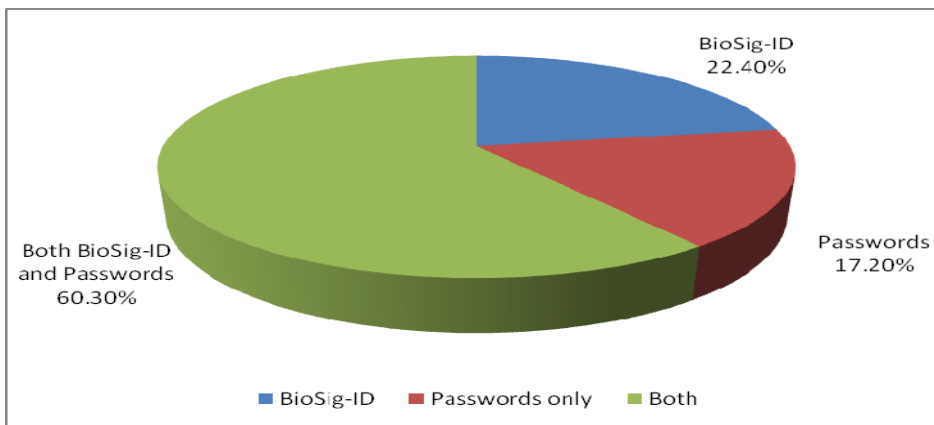


As illustrated in Figure 5: More than 60% of students liked how easy it was to complete the enrollment and validation processes.

A majority of students liked that BioSig-ID provided more protection against identity theft than passwords. Additionally, 50% of students liked that Click-ID was stronger than passwords and 56% agreed that Click-ID avoided help desk calls.

45% of students thought the BioSig-ID system was entertaining.

**Figure 6. Preferred method of login reported by students who completed the pilot.**





As shown in Figure 6, 60% of students who completed the pilot said they would choose both passwords and BSI software (rather than either passwords or BSI software alone) if given the opportunity.

## **Discussion**

The revised education act raises the bar for student verification, with the intent to ensure the academic integrity of students engaged in distance learning. Current methods using pins, userids, passwords, or security questions can fall short of authenticating the “real physical user” and provide less assurance that the students who complete the course or take a computer based exam are who they say they are.

Input from the 58 students who completed the project show broad student acceptance of the BioSig-ID system. These students indicated the instructions were very easy to follow, and they thought the enrollment and validation processes were very easy to complete. Successful communication with students via e-mail campaigns illustrates scalability to a wider audience. No personal identifying information was collected ensuring student privacy.

These results confirm similar pilots published from the University of Maryland University College (UMUC) and University of Texas System Telecampus. Those pilots reported no significant differences compared to this pilot with the 100 students who completed identical surveys and in the audit trails of over 200 students who enrolled and validated. All these results from student populations are very similar to the third party independent testing on the BioSig-ID software completed with 93 temporary workers by the Tolly group.

## **Conclusion**

This pilot study reported that the participants were able to authenticate their identity in seconds using a mouse from any PC, anywhere to establish proof they are who they say they are. The use of gesture/movement software from Biometric Signature ID proved to



be effective in authenticating student ID multiple times during the course over a 67-day period.

The pilot project implemented by Biometric Signature ID and HCC resulted in a high level of acceptance of the BioSig-ID dynamic biometric system. Students who completed the project – enrollment, six validations, and a feedback survey – reported a 98% positive experience with the enrollment and validation processes, as well as the communications and instructions received. Participating students thought the system was very easy to use. They also appreciated its value in increasing security. Enrollment and validation required very little of participating students' time.

Based on the results of this pilot, the BioSig-ID software was well received by users. The high entertainment factor and high user acceptance levels found in this pilot and other pilots suggest future broad success and acceptance by students in a full deployment. This pilot study confirms BioSig-ID can be a valuable tool for remote identity proofing to authenticate student identity. This pilot study also confirmed in this population that BioSig-ID requires little administration, no additional hardware, and can be rolled out using simple e-mail instructions.

## References

- Biometric Signature ID. (2009, Nov 5). Identity proofing for student ID verification: Report of pilot with University of Maryland University College. (0000018 ed.). Dallas, TX: Biometric Signature ID.
- Biometric Signature ID. (2010, Aug 30). Software only biometrics to authenticate student ID-report of pilot with the University of Texas System TeleCampus. (0000020 ed.). Dallas, TX: Biometric Signature ID.
- Biometric Signature ID. (2011, Jan), Ease of use, enrollment, accuracy and protection evaluation. Assessment of the BioSig-ID software with 93 temporary workers. Dallas, TX: Biometric Signature ID.
- U. S. Department of Education,. (2009, Oct. 27 ). *Institutional eligibility under the Higher Education Act of 1965, as amended, and the secretary's recognition of accrediting agencies*. (chap. 74/206) Retrieved Jan. 13, 2011, from <http://edocket.access.gpo.gov/2009/E9-25186.htm>
- McCabe, D. L, and L. Trevino, and K. Butterfield. (2001). Cheating in academic institutions: A decade of research. *Ethics & Behavior*, 11 (3), pp. 219-232.
- McNabb, L. & Olmstead, A. (2009, Jun.). Communities of integrity in online courses: Faculty member beliefs and strategies. *MERLOT Journal of Online Learning and Teaching* 5(10), 208-221. Retrieved Dec. 12, from [http://jolt.merlot.org/vol5no2/mcnabb\\_0609.htm](http://jolt.merlot.org/vol5no2/mcnabb_0609.htm).





- Olson, J. N. & Hale, D.F. (2007, Winter). Administrators' attitudes toward web-based instruction across the UT System. *Online Journal of Distance Learning Administration* X(IV), Retrieved Dec. 11, 2010, from <http://www.westga.edu/~distance/ojdla/winter104/olson104.html>.
- SACSCOC Board of Trustees, (June, 2010). Distance and Correspondence Education - Policy Statement. Retrieved January 17, 2011, from <http://www.sacscoc.org/pdf/Distance%20and%20correspondence%20policy%20final.pdf>. Inline Citation -- (SACSCOC Board of Trustees, June, 2010)
- Stuber-McEwen, D., Wisely, P., & Hoggatt, S. (2009, Fall). Point, click, and cheat: Frequency and type of academic dishonesty in the virtual classroom. *Online Journal of Distance Learning Administration* XII(III), Retrieved Dec. 10, 2010, from <http://www.westga.edu/~distance/ojdla/fall123/stuber123.html>.
- University of Texas System TeleCampus. (n.d.). Data. In *2009 UT TeleCampus annual report*.

*Special thanks to the participating faculty members and their students.*



For more information please contact:

Stephen Levey, Ed.D.  
Associate Vice Chancellor, Academic Instruction  
Houston Community College  
Houston, TX  
713-718-5261  
[stephen.levey@hccs.edu](mailto:stephen.levey@hccs.edu)

or

Jeff Maynard CEO  
Biometric Signature ID  
972-436-6862  
[Jeff.maynard@biosig-id.com](mailto:Jeff.maynard@biosig-id.com)  
[www.biosig-id.com](http://www.biosig-id.com)

## Addendum

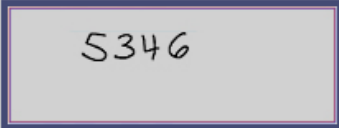
### Enrollment drawing area.

Users “draw their secret code” three times to create a profile

**Enroll BioSig-ID Profile**

**Directions:**

- Select 3 or more different characters/initials/shapes to use as your personal ID (see example)
- Using your mouse, hold the left mouse button down
- Draw these different characters/initials/shapes in the space provided
- Use the lines as the reference
- Select "Next" after completed

**Example:** 

**Success Tips:** Write slow & move your mouse with consistent speed and direction.

	2		9					
		2		0				

Check box to enable invisible ink  
 Uncheck box to remove grid lines

**1 2 3**

Flash Client Version : 1.1

**Clear** **Next** **Re-enroll**

**Click-ID Human Pattern Recognition - serves as the second layer of security**



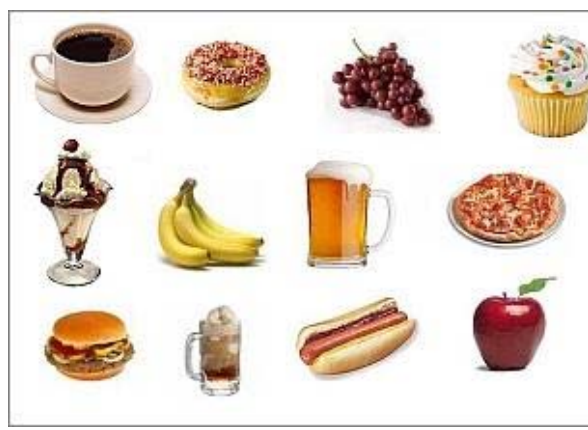
**Kitchen**



**Numbers**



**Retro**



**Food**



## Completion Certificate

