Table of Contents

TABLE OF FIGURES ............................................................................................................................... III
COMPANY BACKGROUND ......................................................................................................................4
SUMMARY OF FEATURE SET ..................................................................................................................5
SECURITY OF INFORMATION TECHNOLOGY .........................................................................................5
THE SOCIAL SECURITY ADMINISTRATION ............................................................................................7
THE FINANCIAL INSTITUTION LETTER (FFIEC, FIL-103-2005) ...........................................................7
ONLINE/DISTANCE EDUCATION NEW MANDATES FOR STUDENT ID VERIFICATION ..................7
HEALTH IT ADVANCED RESEARCH PROJECTS (SHARP)- HHS-2010-ONC-TR-005 .......................7
THE IDEAL SOLUTION DEFINED ................................................................................................................8
FREQUENTLY ASKED QUESTIONS AND ANSWERS ..............................................................................8
  QUESTION 1 – HOW DOES BSI TECHNOLOGY COMPARE TO RISK-BASED AUTHENTICATION
  REQUIREMENTS? ....................................................................................................................................... 8
  QUESTION 2  HOW DO YOUR SOLUTIONS INTEGRATE WITH OUR SYSTEMS? ................................. 9
  QUESTION 3. HOW IS YOUR SOLUTION’S PERFORMANCE, SECURITY, AND RELIABILITY MONITORED,
  MAINTAINED, REPORTED? .................................................................................................................... 9
  QUESTION 4. EXPLAIN YOUR CLOSED LOOP TECHNOLOGY AND HOW IT AVOIDS HELP DESK CALLS
  QUESTION 5. HOW DOES BSI’S SOLUTION COMPARE WITH OTHER BIOMETRIC SYSTEMS? ........... 10
  QUESTION 6. PLEASE COMMENT ON PRIVACY, AND SECURITY VERSUS PINS AND PASSWORDS. .... 11
SUMMARY ..................................................................................................................................................12
  GENERAL DATA SHEET BSI ..................................................................................................................12
INTRODUCING BIOSIG-ID™ - DYNAMIC BIOMETRICS ........................................................................13
  TWO FACTOR AUTHENTICATION IN ONE .......................................................................................... 13
  REVOKE AND REPLACE ....................................................................................................................... 14
  HOW DOES BIOSIG-ID™ WORK? ......................................................................................................... 14
  AUDIT TRAILS ....................................................................................................................................... 14
  CLOSED LOOP ..................................................................................................................................... 15
INTRODUCING CLICK-ID™ TECHNOLOGIES FOR IDENTITY VERIFICATION .............................16
ABOUT THE FOUNDER ............................................................................................................................18
Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Drawing area and secret code used with BioSig-ID</td>
<td>13</td>
</tr>
<tr>
<td>Figure 2</td>
<td>BioSig-ID secret code examples</td>
<td>14</td>
</tr>
<tr>
<td>Figure 3</td>
<td>BioSig-ID Audit Trail Log Report</td>
<td>15</td>
</tr>
<tr>
<td>Figure 5</td>
<td>Click-ID picture examples</td>
<td>17</td>
</tr>
<tr>
<td>Figure 6</td>
<td>Click-ID image distortion</td>
<td>17</td>
</tr>
</tbody>
</table>
Company Background

Biometric Signature ID (BSI) is a four year old software development company based in Dallas Texas. We have no subsidiaries and are privately held. We specialize in identity and access management solutions, the core of which is our patented biometric signature/gesture technology. We hold one recently issued patent and have one patent pending. We also offer an online signature product, Sig-ID Online™ that allows any contract/form to be signed virtually over the Internet using their mouse. This product conforms to the e-Sign laws and equals a “wet signature” completed with pen and paper. In addition, BioSig-ID WinLogon™ provides our dynamic biometric signature gesture solution authentication before the user can access their Windows screens. Our products span multiple verticals including government, healthcare, cloud computing, online banking, distance education and more.

We offer the following software solutions for identity management with remote users:

1. **BioSig-ID™** - Dynamic biometric signature /gesture identity authentication
2. **Click-ID™** - Human pattern recognition technology for strong identity verification
3. **Complex Security Questions** – Verify the user through questions and answers

All solutions require no hardware, have multiple levels of security that can be activated and provide seamless integration with a “closed loop” self service password reset. This provides the maximum security and flexibility for users.

Our premier patented biometric dynamic signature/gesture solution BioSig-ID uses your “mouse” to positively authenticate the physical user. BioSig-ID captures HOW a person writes/draws (speed, length, height) which are behavioral characteristics unique to each individual. These unique biometric characteristics cannot be borrowed, duplicated or shared and represent the highest level of identity authentication and security.

Initial enrollment takes minutes with validation against their stored profile taking seconds. Even if someone was to find out your code they must complete an extra step: duplicate your unique code to authenticate themselves as the real user - an impossible task! BioSig-ID makes the risk of easily guessed or weak passwords or knowledge questions irrelevant and stolen credentials completely worthless.

Our Click-ID solution provides identity verification using your “mouse” to click on the correct image, the correct three objects, and the correct order of these objects. Initial enrollment is at the same time as BioSig-ID. Enrollment profiles are kept in a secure database. In validation if the selections are correct, access is granted. Images are randomly altered on the page to prevent machine generated bot attacks and act as a one time password. Click-ID replaces security questions, tokens, smart cards, images, IP addresses, device reputation or biometrics that require hardware.

Complex Security Questions are used as an alternative access system with Click-ID only when a student has difficulty with a mouse. The same closed loop technology is built into this Click-ID and Complex Security Question access “tree”.
In a recent pilot with University of Maryland University College (UMUC), students were able to enroll in 1.5 minutes and thereafter validate their identity at periodic challenges in approximately 20 seconds each.

Summary of Feature Set

Biometric Signature ID offers a unique signature/gesture biometric and identity management technology that provides the following advantages over other dynamic solutions, hardware based solutions or question based technology:

- NO Hardware required – eliminates cost and scalability issues
- Authenticates the physical user, versus questions that only assert an identity
- 93% of users find it “Extremely or Very Convenient” to use
- Little administration required
- Instantly scalable, any PC anytime, anywhere
- 100% enrollment (fingerprint biometrics have a failure to enroll up to 3%)
- Age and language independent
- Audit trails tracks event and session records
- Audit trail information can be used for data mining purposes
- Unique closed loop that creates automatic password reset and allows continuity
- Accepted by biometric experts, proven, accurate and reliable
- Random periodic challenges during the session allows user authentication along multiple points of contact to ensure identity

Security of Information Technology

Information security is a cornerstone of achieving nationwide exchange and use of electronic digital asset information. Without security there can be no trust. Without trust, we cannot have successful IT adoption or information exchange. Without adoption and exchange we cannot achieve the improved security and outcomes we want and need.

DHS’s operational biometric systems currently contain more than 100 million records and are anticipated to approach 500 million records, yet these databases are unavailable to the research and development community due to privacy concerns and security restrictions imposed on the data. The major challenges requiring breakthrough product solutions include the development of security functions, policies and technology tools that will facilitate increasingly widespread, rapid, and sophisticated, electronic use and exchange of IT information while assuring and enhancing individuals’ safety and privacy.

Biometric Signature ID (BSI) is committed to meeting growing demands by providing secure, reliable, and efficient delivery channels for transacting communication and business electronically. We offer a unique NO HARDWARE and NO INSTALLATION approach. As electronic communication continues to grow through networks or through accessing data in the cloud users must participate in an identity and access management process.
The consequences of personal health information security breaches, that can lead to identity theft and mis-use is best summarized by Ex DHS Secretary Chertoff:

"I'm going to submit to you that in the 21st Century, the most important asset that we have to protect as individuals and as part of our nation is the control of our identity, who we are, how we identify ourselves, whether other people are permitted to masquerade and pretend to be us, and thereby damage our livelihood, damage our assets, damage our reputation, damage our standing in our community."

DHS Secretary Chertoff Addresses Secure Identity Challenges

The problem that government, institutions, and merchants face is Internet identity authentication during secure transactions. Current Identity proofing methods do not identify the physical user. They are typically centered on predicting identity or behaviors, based on whether the user is who they say they are, because they possess knowledge that is supposed to be known only by the individual (Pins or passwords) OR they verify that a piece of hardware (i.e. tokens) is working and assumes it is in the hands of the intended user.

However with the Internet’s wide appeal comes the ability to easily uncover most of a users’ personal credentials, including but not limited to: history, DOB, address, SSN, and virtually all of their healthcare and financial information. Identity theft is now one of the fastest growing crimes and this has affected consumer behavior to request higher standards of privacy protection.

This information is obtained through simple searches using the common Internet search engines, reference web sites, social web sites, personal blogs, and so forth.

More direct attacks to harvest information using strategies such as malware, bot networks, phishing, social engineering attacks, and Trojans produce information that can be easily harvested by hackers to commit identity theft and fraud.

It is estimated that 83% of all computers are infected with Trojans, key loggers, or malware that collect and transmit data that includes PINS, passwords, bank account numbers, and other personal identifiers for user accounts, back to a remote master server which could be located anywhere in the world. In addition to hackers, PIN’s, passwords, smartcards, and tokens can be stolen “or borrowed” by colleagues. Such data which includes healthcare data, customer lists, corporate trade secrets, and account access information, on the black market’s buy and sell web sites, gross over $26B in revenue yearly.

IT departments try to counter these security threats by having users create longer passwords, change passwords every 3 months, provide education, add security questions, etc. Users typically have difficulty remembering the myriad of password changes, verification questions, etc. and have to write them down, seriously increasing
the risk of compromise. This in turn becomes counter productive, as customers simply will not use e-commerce sites if they become too difficult or frustrating to access. In particular, this could be a significant obstacle for persons that are more elderly.

Like PINS and passwords, answers to questions or about images are very vulnerable to social engineering and on-line hacking methods. The Web is now the primary conduit for hackers with nearly 50% of all fraud being carried out using the Internet.

The following areas are indicative of the need for higher multi-factor authentication security, acknowledging why PINS and passwords are no longer sufficient as single credentials.

The Social Security Administration
In their recent RFP- Reference: SSA-RFP-09-1058. Titled “Authentication and Identity Proofing Data Source” they intended to “expand E Authentication protocols to allow for more complex transactions via automated applications and enhance service delivery”, for their 53M client users. They required Level 3 NIST compliance, where identity proofing procedures require verification of identifying materials and information. A minimum of two authentication factors is required to determine the identity of a user before gaining access to data files.

The Financial Institution Letter (FFIEC, FIL-103-2005)
“Authentication in an Internet Banking Environment.” For banks offering Internet-based financial services, the guidance describes enhanced authentication methods that regulators expect banks to use when authenticating the identity of customers using on-line products and services. They proposed that Biometric identifiers are most commonly used as part of a multifactor authentication system, combined with a password (something a person knows) or a token (something a person has). They described the various biometric techniques and identifiers being developed and tested, that included: fingerprint recognition; face recognition; voice recognition; keystroke recognition; signature/gesture recognition; finger and hand geometry; retinal scans.

Online/Distance Education New Mandates for Student ID Verification

(g) Requires institutions that offer distance education or correspondence education to have processes in place through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the course or program and receives the academic credit.

Health IT Advanced Research Projects (SHARP)- HHS-2010-ONC-TR-005
In this American Recovery and Reinvestment Act of 2009, they are looking for research to address the challenges of developing security and risk mitigation policies and the technologies necessary to build and preserve the public trust as health IT systems become ubiquitous. Areas of concern include:
• Consumer access and control: addressing consumer concerns regarding timely access to their own data and how their health data is shared and, potentially, their perceived lack of consumer control
• Data Access: to only those who need access for care delivery;
• Data breaches
• Data stewardship and the ability to assure minimum necessary access and appropriate use of patient data

Information is a most precious asset. Information technology should be using the highest most secure approach to safeguarding its digital assets and this is by multi-factor authentication. It is not always possible to use a token, biometric readers or other hardware approaches to validate a users' identity. We offer a different approach to authenticate the user's identity without hardware that requires no installation.

The Ideal Solution Defined

Biometric Signature ID offers a new and very unique patented solution. Our dynamic biometric identifies a person based on their behavioral characteristics that are unique to each person, that are impossible to duplicate or share. Our technology stops fraud as only users who authenticate their identity can access personal files, their PC or web sites online. We do this without hardware and without the need for installation.

Clients use only a “mouse” stylus or touchpad to activate the system and create a profile. The system does not use “cursive signatures”. Rather, users will choose something of meaning to them and this could be letters, numbers or shapes. In this way the system is age and language independent. Unlike other biometrics, BSI created a solution that involves biometrics combined with a multiple layer of security unique to BSI. BSI technology offers multi-factor authentication in one solution as it combines signature/gestures, image pattern recognition and complex security questions. This solution is called a “closed loop” technology and it offers one of the highest levels of identity proofing and management available. BSI technology is best suited for remote access over the Internet or for access to the users computer.

We have developed a series of frequently asked questions and how BSI technology addresses key elements of an ideal solution.

Frequently asked Questions and Answers

**Question 1 – How does BSI Technology compare to Risk-Based Authentication requirements?**

Risk based authentication (RBA) is used when the identity of a person cannot be definitely established and provides a real time assessment of the validity of an asserted identity. This strategy does not authenticate the physical user. They cannot discriminate whether the user is the real person and only assert that the user knows the answer to a question. If someone knows the answers to the questions they can masquerade as another. These questions fall short of being a single credential for identity validation in any multi-factor authentication strategy. If they are to be used they must be used with something that “you are” and this is always a biometric.
Biometric Signature ID (BSI) technology on the other hand is the only dynamic biometric that can establish the identity of the person online using multiple security layers after they have enrolled a profile into the Biometric Signature Registry (BSR) secure database. The BSI solution supports customer registration and subsequent authentication events.

BSI technology produces a definite positive identity of the person through the use of our dynamic signature /gesture biometrics. Using our technology a person enrolls a profile by signing three times with their mouse of other pointing device. This profile contains UNIQUE characteristics of how the person draws/signs with their mouse (or other pointing device like touchpad, stylus). The biometrics characteristics include speed, direction, angle, length and other indices. After the person has enrolled they are asked to authenticate their identity and their new signature is compared to the profile kept in the database. If the new signature falls within a “threshold” the person’s identity is verified and they can move to the next step. The threshold can be adjusted to create different levels of security based on a risk generated score of the digital assets to be accessed.

Our technology can be used with out of wallet type strategies to establish a high level of assurance the person is who they say they are, especially important for first time users. For multiple use persons accessing online records, our solution(s) can be used singularly as they provide the highest level of identity proofing available online and offers both multi-factor authentication and 4 layer security.

The BioSig-ID Online, Click-ID Online and Complex Security Questions architecture consists of three (3) layers of security. During enrollment, a user enrolls in a minimum of 2 security methods consisting of a primary and alternative access method. If a user is unable to enroll in the primary access method for any reason, the alternative access method defaults to become the primary and the third alternative access method becomes secondary. This provides maximum security and flexibility for users. The alternative access is also a profile re-set technology, helping avoid help desk calls in the event they "forget" their primary access method. We are uniquely qualified to offer this closed loop solution.

**Question 2  How do your solutions integrate with our systems?**

The BSI technology is a client server communication scheme (Figure 1). It involves the use of a client’s PC, a web server (hosted by you the client) and a BSR server. Since our technology sits in front the configuration it allows for the use of all major operating systems and browsers. We employ the use of a Flash component which is resident in 99+% of all PC’s. The user does not have to install or download any software or use any special hardware. The BSR server is also located behind the client’s firewall, affording the highest level of security. BSI provides a solution that is always available and has an immediate response time.

**Question 3. How is your solution’s performance, security, and reliability monitored, maintained, reported?**
The BSI technology tracks all identity verification activity in “audit trails” (Figure 2). The audit trail functions to provide the following benefits:

- They record the success or failure of the individual to log in, time to complete the enrollment or identity verification, whether non approved web IP addresses have attempted to access the system, what BSI systems the user accessed (we have multiple layers), time and date stamps, what IP address was used, and with some of BSI’s solutions the unique session ID and unique ID assigned to the user.
- The audit trail provides the administrator ability to search for an individual’s activity access information OR a search by time period OR group can be completed.
- The audit trails can be configured to produce standard or custom reports for the administrator.
- Provide management information (MI) data reports:
  - Make available MI data reports per: day, week, month, and year
  - Week: include daily MI and weekly summaries
  - Month: include monthly summaries
  - Annual wrap-up
- Audit trails include:
  - usage statistics
  - matching statistics (successes & failures, per data element)
  - verification failures
  - out-of-wallet failures
  - fraud indicator report
  - trend reporting
- The BSI solution maintains a seamless experience for the user while not requiring a significant change to the end users’ Web application experience. Nothing is installed or downloaded.

**Question 4. Explain your closed loop technology and how it avoids help desk calls**

The BioSig-ID, Click-ID and Complex Security Questions architecture consists of three (3) layers of security. During enrollment, a user enrolls in a minimum of 2 security methods consisting of a primary and alternative access method. If a user is unable to enroll in the primary access method for any reason, the alternative access method defaults to become the primary and the third alternative access method becomes secondary. This provides maximum security and flexibility for users. The alternative access is also a profile re-set technology, helping avoid help desk calls in the event they "forget" their primary access method and is unique to our solutions. This feature significantly reduces the resources required to support the technology.

**Question 5. How does BSI’s solution compare with other biometric systems?**

a. Static biometric like fingerprints, facial scans etc. require the use of costly hardware. This hardware requires mailing, training and maintenance adding costs and reducing scalability. Fingerprint readers have been known to range in
effectiveness from only 30% to 99.9%, which is why they have not been adopted in airports – you need to pull people out of line to process manually. In addition there is a failure to enroll with fingerprint readers up to 3%. This means up to 3% of people will not be able to enroll in the system and a back up plan is required.

b. Dynamic biometrics like voice and keystroke while offering certain advantages over static biometrics do not measure up to signature gestures due to: voice has limited application to authenticate identity. Keystroke captures only one biometric index-time between strokes which limits its authentication reliability and requires users to enroll up to 20 times. Keystroke programs usually have to involve additional risk based authentication systems to increase their reliability.

c. BSI requires no additional hardware and reduces costs while increasing scalability. BSI uses a “training enrollment” that offers a 100% enrollment. Since the user is in control of what they draw/write or select they have little of no issue in producing 100% effectiveness. BSI’s BioSig-ID requires the user to enroll only 3 times and collects up to 6 biometric indexes for maximum reliability and effectiveness.

d. Dynamic biometrics like BSI’s signature gesture technology are Multi-factor authentication by itself. The use of what you sign is the first factor “something you know” and the signature or code is “something you are” = the second factor. This is unique to dynamic versus static biometrics. BSI goes even further to create a four level security:

- Use of a reference ID = something you know
- Choose your secret code = something you know
- Draw or sign your secret code = something you are
- Choose objects using Click-ID = something you know

e. BSI technology works as an integrated system and provides for Identification, Authentication and Authorization, a first for a biometric.

f. Enrollment usually takes 2 minutes and validation takes only seconds, almost the same time it takes to type in your hardened password.

**Question 6. Please comment on privacy, and security versus PINS and passwords.**

a. BSI biometric solutions are unique to each individual and cannot be lost, stolen, or borrowed compared to Pins, passwords, tokens, cards and other security solutions. If I know your PIN for example it is a 100% security failure and is unacceptable as the single point of identity validation in today’s environment. This failure is why the federal government mandates multi-factor authentication for online banking and more.

b. One key element of collecting biometric data is privacy. If your fingerprint is hacked from a database it is gone forever. With dynamic biometrics we have advantages called Revoke and Replace. This means that the dynamic signatures you make can be instantly revoked and you can always create a new one in any event where the database might be compromised. This is only true for dynamic biometrics.
Summary
Proper security controls and robust e-authentication provides reliable and accurate identity verification outcomes for citizens, businesses and other government agencies which rely upon IT communication. The technology must be scalable, offer multi-factor authentication, easily revoked and managed and NOT collect personal identifying information on its users. Biometric Signature ID technology meets these goals.

For any additional information please contact the undersigned. With regards,

Jeff Maynard

Jeff Maynard
President and CEO
Biometric Signature ID, www.biosig-id.com, 972-436-6862, 214-244-7679 cell

General Data Sheet BSI

a) Name of Vendor: Biometric Signature ID (BSI)
b) Address: 708 Valley Ridge Circle Suite 8
c) City, State, Zip: Lewisville, TX 75057
d) DUNS Number: 784074911
e) TIN: 75-2636859
f) CCR Registration Confirmation Number: 5UDW7
g) NAICS code: 541511
h) Small business designate
i) Point of Contact: Mr. Jeff Maynard, CEO
j) Telephone Number: 972-436-6862
k) Fax Number: 972-317-2184
l) Electronic Mail Address: jeff.maynard@biosig-id.com
Appendix 1

Biometric Signature ID - Product Review

Introducing BioSig-ID™ - Dynamic Biometrics

BioSig-ID is a patented product using unique Dynamic biometric handwriting & gesture technologies. Activation is from any mouse, stylus or touchpad on any PC anywhere, anytime. BioSig-ID captures HOW you write/draw including your speed, direction, width, angle and length which is unique to each individual. The software allows access to only registered users who authenticate themselves against a stored profile. Users enroll one time and thereafter validate their identity in seconds.

Two Factor Authentication in One

BioSig-ID is a proven two factor solution to user authentication and with unique biometric data it cannot be lost, stolen or forgotten like PINS, tokens, cards and passwords. In an increasingly regulated market BioSig-ID provides a low cost, instantly scalable identity management solution for both the desktop and browser based account access.

Unlike finger, retinal or face scans only Dynamic biometrics allows the enrollee to introduce a secret code into the biometric process. The users can enroll with “a code or drawing” of their own choice which is their secret code (Figure 4).

![Figure 1 Drawing area and secret code used with BioSig-ID](image)

Dynamic biometrics combines secrets with biometric samples (your unique way of drawing for example) to provide two-factor authentication in one process. BioSig-ID goes further than other static or dynamic biometrics because BioSig-ID is a unique 4 layer authentication that requires no special hardware:

Use of a reference ID = something you know
Choose your secret code = something you know
Draw or sign your secret code = something you are
Choose objects using Click-ID = something you know
**Revoke and Replace**

Only Dynamic biometrics allow an infinite number of different secret biometric samples (codes, images, and numbers) generated by the same individual. Revocation is instant and replacement is only a re-enrollment. If your fingerprint gets hacked it is gone forever. With BioSig-ID you can always change your drawing behavior.

**How Does BioSig-ID™ Work?**

Enroll (one time only) in the drawing area three times. Your enrollment “profile” is kept in a secure database and when you validate, your signature is compared to your “stored profile”. If it falls within a certain threshold, access is granted. Click-ID Image Technology creates an alternative access method and is strong authentication by itself. There is always a two layer approach using a primary and alternative access method for maximum flexibility and security. The alternative access is a profile re-set technology, that helps avoid help desk calls and is unique compared to all other biometrics.

![Draw your “Secret Code”](image)

**Figure 2 BioSig-ID secret code examples**

**Audit trails**

The BSI technology tracks all identity verification activity in “audit trails” (Figure 3). The audit trail functions to provide the following benefits:
They record the success or failure of the individual to log in, time to complete the enrollment or identity verification, whether non approved web IP addresses have attempted to access the system, what BSI systems the user accessed (we have multiple layers), time and date stamps, MAC address trace, what IP address was used, and with some of BSI’s solutions the unique session ID and unique ID assigned to the user. The audit trail provides the administrator ability to search for an individual’s activity access information OR a search by time period OR group can be completed. The audit trails can be configured to produce standard or custom reports for the administrator.

---

**Audit Trail**

**BIOSIG-ID AUDIT TRAIL LOG ANALYSIS**

Session Report for User ID: student123@utsystem.edu from November 23, 2009 00:00:00 a.m. to November 24, 2009 11:59:59 p.m.

- **Session #1**: Enroll BioSig-ID as the Primary Access Method.
  - (Begin on Nov. 23, 2009 09:09:50 a.m.)
  - Step 1: 1st attempt is submitted at Nov. 23, 2009 09:09:50 a.m. -> Success.
  - Step 2: 1st attempt is submitted at Nov. 23, 2009 09:10:16 a.m. -> Success.
  - Step 3: 1st attempt is submitted at Nov. 23, 2009 09:10:28 a.m. -> Success.

- **Session #1**: Enroll Point & Click Image (PCI) as the Alternative Access Method.
  - (Begin on Nov. 23, 2009 09:11:10 a.m.)
  - Step 1: 1st attempt is submitted at Nov. 23, 2009 09:11:10 a.m. -> Success.
  - Step 2: 1st attempt is submitted at Nov. 23, 2009 09:11:21 a.m. -> Success.
  - Step 3: 1st attempt is submitted at Nov. 23, 2009 09:11:28 a.m. -> Success.

Session Summary Report for User ID: student123@utsystem.edu from November 23, 2009 00:00:00 a.m. to November 24, 2009 11:59:59 p.m.

- **Session #1**: Enroll Point & Click Image (PCI) as the Alternative Access Method.
  - (From Nov. 23, 2009 09:09:34 a.m. to Nov. 23, 2009 10:43:63 a.m.)
  - -> Primary Access Method w/ BioSig-ID Enrollment: 3 signatures -> Success.
  - -> Alternative Access Method w/ PCI Enrollment: 3 -> Success.
  - -> Primary Access Method w/ BioSig-ID Validation: 1 signatures -> Success.
  - -> Alternative Access Method w/ PCI Validation: -> Success.

Figure 2 BioSig-ID Audit Trail Log Report

**Closed Loop**

To avoid helpdesk calls and to allow the client to have a positive user experience, BSI created a patent pending closed loop technology. One of the largest issues facing merchants who deliver web based services is what happens when the client forgets their password? On average a call for password re-set costs up to $21 per call. BSI created a solution where the client who cannot authenticate their identity can still be verified and continue without a help desk call. The client who fails to authenticate is directed to their secondary profile which is stored in the secure database. This profile is one of two that is created in the initial registration and enrollment phase. If the client is able to verify themselves using Click-ID (against their stored profile) they are directed to re-enroll their BioSig-ID profile. Alternatively, the administrator can allow the client to proceed with a BioSig-ID re-enrollment. This system accounts for users who may not be frequent
visitors to the site and may not remember their BioSig-ID secret code or how it was written say a year ago.

**Closed Loop Technology—always 2 levels of security**

![Image of BioSig-ID Closed Loop Technology]

**Figure 4 BioSig-ID Closed Loop Technology**

**Introducing Click-ID™ Technologies for Identity Verification**

Provides patent pending identity verification using images that are chosen from a list. After you choose an image the user must select specific objects in the image and in a sequence they must remember. Their identity is verified against a stored profile completed during enrollment. Enrollment profiles are kept in a database as binary code and used to compare to a new selected image and objects. If the selections are correct, identity is positive and access is granted. Every image that is presented after enrollment is changed so the user must remember what objects they selected and in the correct order. **Each identity validation is randomly changed and acts as a one time password, a strong defense against duplication, bot attacks and hackers.**

No need for any special equipment or hardware, just a mouse, stylus or touchpad. Audit trail log creates compliance document for multi-purposes. Application is for any browser based systems. Replaces tokens, smart cards, images, IP addresses, device reputation or other biometrics that require hardware. Augments PINS and passwords.

Click-ID by itself is stronger than a “hard” password or complex questions and infinitely easier to use as it requires only clicking on specific objects to verify the user’s identity. BioSig-ID combines with patent pending Click-ID™ Image technology that creates an alternative access. Click-ID by itself is stronger than a “hard” password (8 characters)
but infinitely easier to use as it requires only clicking on objects to verify the user’s identity.

**NEXT STEP:** BioSig-ID Technology allows you to create an alternative access for your personal protection and flexibility.

**Direction:** Please click on an image below to begin.

![The Numbers](image1.png)  ![The Animals](image2.png)

![The Bedroom](image3.png)  ![The Kitchen](image4.png)

**Figure 5 Click-ID picture examples**

**Direction:** Please click on the center of the objects in the same order that you selected during enrollment.

**Note:** Image may change slightly from the original form.

![Image Distortion](image5.png)

**Figure 6 Click-ID image distortion**
About the Founder

Mr. Maynard is the CEO and founder of Biometric Signature ID. He is the creator of several patented and patent pending inventions using handwriting biometrics and image pattern technologies to verify identity. He is a former CEO running 2 divisions using biometrics in healthcare for a public traded company. Previously Mr. Maynard was a partner in a software firm that created predictive modeling software for large healthcare clients like United Healthcare. The company was sold to a public company. Mr. Maynard received his undergraduate degree from York University, Toronto and completed executive training from Harvard/MIT, and Kellogg School of Business. He is a committee member for the INCITS/NIST “Study Report on Biometrics in e-authentication 2007, member of Center for Ethical Identity Assurance (www.ceiaglobal.org), volunteer for the Biometric Technology Working Group for the National Biometric Security Project. Mr. Maynard has been a guest lecturer at University of Texas, Dallas Business School, a judge for the UTD Business School Idea Competition, a keynote speaker at 3 conferences, has been an invited speaker at the Texas Technology Executives Network, the Technology Executive Network Group, MIT Enterprise Forum and is a co-star presenter at UNT division of MIS graduate studies. He has published selected works on biometrics including in the trade journal - Smart Card and Identity News entitled “Click Click Who’s There?” white papers “Student ID Identity Proofing Solutions” “Internet Based Identity Proofing”, and is a sought out speaker on the application of Dynamic biometrics.