November 2007 Volume 16 • Number 11

Smart Card & Identity News

Smart Cards, SIM, Biometrics, NFC and RFID

www.smartcard.co.uk

*Jeff Maynard*

# "Biometric Signatures for Identity Authentication and Reduction of Identity Theft"

Jeff Maynard CEO/Founder Biometric Signature ID (Dallas Texas)

## Click, Click Who's There? - An Identity is stolen every 79 seconds. (excerpt from Smart Card and Identity News)

Identity theft is increasing rapidly. Over 214M Americans have had their personal information exposed to the world since 2005[1]. This data is stolen using any of the five common ways such as phishing scams, viruses, database hacking, stolen laptops, thumb drives or CD's, or from insider theft. This information can include your social security number, address, DOB, insurance information, credit card information, PINS and passwords or bank accounts.

The scary part is what happens with this personal data? It is called Identity fraud. This is when individuals use another's identity for misrepresentation leading to criminal activity. A criminal in possession of your personal data is free to write checks, apply for credit cards, access your bank accounts, apply for loans and more. We cannot stop identity theft but we can reduce identity fraud by reducing the access using biometrics.

In the US nearly $50B in annual losses result from identity fraud [2]. This is a serious number. Utica College and the secret service recently found that the total cost of each incident of identity fraud is $31k and that the Internet is the enabler in nearly 50% of cases. There is a huge underground economy where credit cards can be bought for $490, drivers' licenses for $147 or social security numbers for $98.


It is estimated the malware (fraud) industry is greater than $26B annually, more than the revenue from legit security vendors. Hacking is so easy that we no longer know how much has been hacked. Is it 40M credit card numbers or is it 94M that got exposed at TJMAXX?

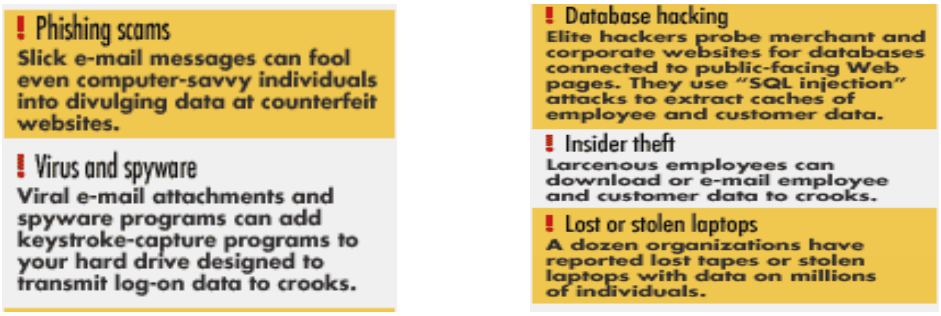
Most organizations and their security guru's believed in the "security cocktail" of products, including virus scanners, firewalls, spyware detectors, penetration detectors, and filters to protect that information from internet hackers. More recently they have relied on behavior patterns, online IP addresses, multi layers of security, secure –ID tokens or the selection of site images. As reported by Dark Reading Aug 2007, research outlined a variety of methods that attackers used to turn banks' latest security measures (images, more questions) to their own advantage and this

contributed to a pump and dump scheme netting over $22M with two popular brokerages. In a virtual world you need to know who the person is not what computer, token or password they use. Relying on these security cocktails is simply not working.

## Understanding access

To understand identity fraud we must understand how identity theft works. Table 1 looks at the most common ways personal data is obtained. If a hacker can place a Trojan in your computer there's very little you can do. Clever phishing scams have tricked an estimated 15M computers to upload the Storm Virus to form a huge Botnet, to conduct malicious criminal activity. In a more recent case specialized code was created to run a scam called the fake FTC virus attack. This sophisticated attack used information from previous data thefts to target individual e-mail users including a well known sales management company. A far higher percentage of recipients actually open the poisoned attachments and forwarded them on.

### Table 1- How Identity Theft Occurs




## Factors affecting behaviors

We need to find better security solutions but human behavior needs to be nudged into taking action. ChoicePoint's $15M fine along with other companies[3] have been fined and had to agree to FTC oversight for 10-20 years for their data breaches. In addition the cost of complying with breach notification laws was estimated at $14M per company[4]. HIPAA breaches have already sent people to jail with more fines and job losses imminent. The following laws are a call to action.

> 35 state privacy laws, SOX, DHS, GLBA, FFIEC, HIPAA, PIV, Specter-Leahy Data Privacy Act, Online Child Protection Act, Social networks pending regulations, Payment Card Industry (PCI), 21 CFR Part 11, Bill 198 Canada, ISO 7099 Best IT practices…

A very serious precedent setting lawsuit involved a physician who gave his PIN/password to a staff member to access Protected Health Information (PHI) [5]. The staff member was also a patient and accessed PHI including his own for a year. He became distraught and sued the physician using HIPAA as the "new standard of care". The State Appellate Court agreed and the precedent has been set. Any entity that manages PHI or personal identifiers (nurses, school counselors, trainers, benefits managers etc.) may now be considered a "covered entity" susceptible to similar law suits.

If we combine all the factors: huge continuing identity fraud losses due to inadequate technology, fines, high costs to repair identity fraud, high costs of announcing and fixing identity theft for companies, new laws to protect against terrorists and secure our borders and loss of revenue from users who refuse to buy online etc. the environment is changing quickly to new security methods.

## Biometrics to solve the crisis

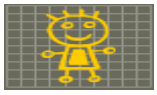
Clearly a solution does not exist that combines identification, authentication and authorization of unique users in a practical, scalable fashion.

Passwords and PINS can be acquired by direct covert observation. Once an attacker acquires the user ID and the password, the intruder has total access to the user's resources. There is no way to positively link the usage of the system to the actual user; and no protection against repudiation by the user. When a user ID and password is shared with a colleague, there is no way for the system to know who the actual physical user is. A similar situation arises when a transaction involving a credit card number is conducted on the internet. If you illegally downloaded music using a friends' password, your friend could be the one fined and jailed. Even data sent using secure encryption methods, cannot assure that the transaction was initiated by the rightful owner of the credit card, token or smart card. It is not yet cost effective to issue tokens or other hardware and readers to the masses in remote e-authentication environments. Dynamic biometrics require no additional hardware and are ideally suited for this application.

In the United States, 69% of citizens want banks, credit card companies, health care providers, and government agencies to adopt biometric technologies, ahead of other security technologies like smart card readers, tokens and passwords. In the UK, the number is higher, coming in at 92%. (Information Week Feb 6, 2007 Ponemon Institute)

Biometrics is a rapidly advancing field that is concerned with electronically identifying a person based on physiological or behavioral characteristics. Automated biometrics include: fingerprint, face, iris and signature/gestures. A biometric property is an intrinsic feature of an individual and is difficult to duplicate and nearly impossible to share. There is no universal biometric for all needs but in the remote authentication environment Dynamic biometrics should form the common denominator in a multi-factor authentication strategy where 2 of 3 factors are chosen and where a biometric always forms one of these factors as described:

### Table 2- Multi-Factor Authentication

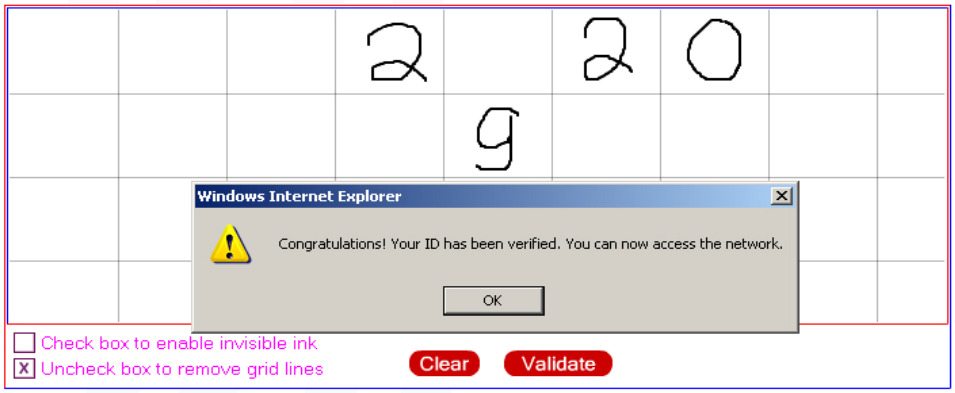
| | | |
|---|---|---|
| 1. Something you **Have** |  | *Credit card, Tokens, Smart Card, device* |
| 2. Something you **Are** |  | *Unique biometric characteristics* |
| 3. Something you **Know** |  | *PINS, password images* |

## Introducing BioSig-ID™ - Dynamic Biometrics

BioSig-ID patent pending suite of products are 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, 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. 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.

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.

## Figure 1- Drawing area and secret code used with BioSig-ID




## Two Factor Authentication in One

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 “drawings” of their own choice which is their secret code (Figure 1).

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:

BioSig-ID is 4 layer authentication that requires no special hardware:

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

## Revoke and Replace

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.

## Other benefits of BioSig-ID products:

- User friendly, instantly scalable
- Use of invisible ink to avoid “shoulder surfers”
- A training site to certify users/employees before going live
- Adjustable security levels (1-99)
- Always a two level solution with a primary and alternative access

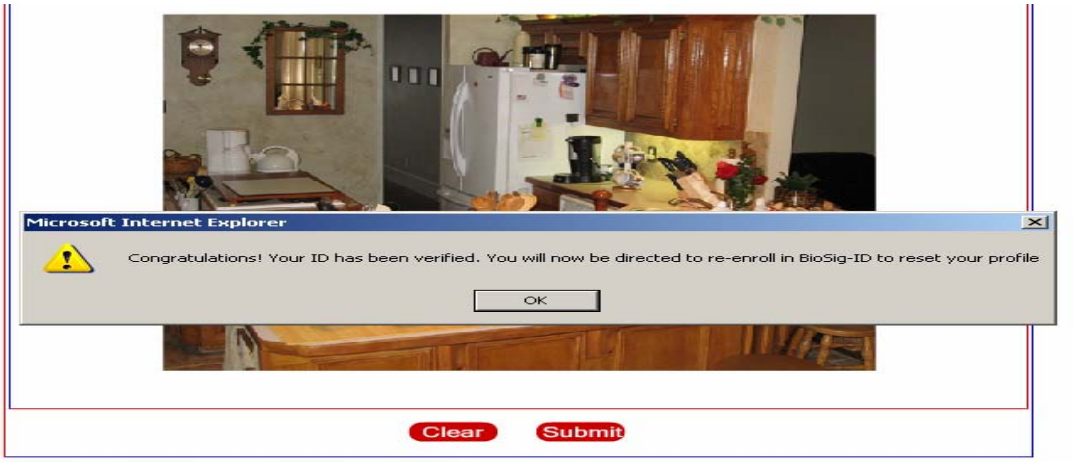
- Age and language independent
- Two biometric products- BioSig-ID Online, BioSig-ID WinLogon
- Three hardened verification products -Click-ID Online, Click-ID WinLogon, Click-ID Reset
- One product to demonstrate strong evidence of ownership - Sig-ID Online
- Administrative console tracks event and session records
- Up to 4 profiles per user allows multiple pointing devices (mouse, stylus, touchpad).
- Knowledge based questions form additional access alternative
- No hardware required
- Machine driven attacks become impossible
- Proven, accurate and reliable
- Enroll in minutes, validate in seconds

## 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 should help avoid help desk calls and is unique compared to all other biometrics..

## Figure 2 – Click-ID™ Personal Images Build a Profile

**Figure 3 – Click-ID™ Alternative Access Method**




## Multi-modal approach

Dynamic biometrics for authentication in open networks, for the desktop and soon cell phones offers the promise of secrecy, privacy, revocation and user friendliness. No hardware requirements allow instant scalability to form the core of any multi-factor authentication solution in selected environments. A centralized approach for credit card processing is also an excellent approach when combined with Dynamic biometrics or other identity control methods like Click-ID. If a user has to authenticate their identity before a credit card transaction is completed/accepted the opportunity for criminals to commit identity fraud in the virtual world can be significantly curtailed. The resulting savings to consumers, online merchants and credit card companies is huge.

It is clear that PINS and passwords are not enough to control un-authorized access in the virtual world. Users want more secure methods, yet not everybody is ready to move to a Dynamic biometric yet. This is why BSI has created multiple solutions from stronger to strongest because it is all about choices.

## Summary

Biometrics offer the best defense against identity fraud as they cannot be stolen, borrowed or forgotten. For the remote environment like logging in to your Internet account or onto your PC, a dynamic biometric like BioSig-ID can provide the solution to controlling identity fraud by restricting access to only registered users who authenticate themselves. Even if the “bad guys” obtain your personal information they would have to authenticate “your” identity before being allowed access. Insist that your place of business uses a biometric before it is too late!

## About the Author

Mr. Maynard is the CEO and founder of Biometric Signature ID. He is the creator of several patent pending inventions using handwriting biometrics and click technologies to verify identity. He is a former CEO running 2 divisions using biometrics in healthcare for a public traded 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, has published selected works on biometrics and is a sought out speaker on the application of Dynamic biometrics.

References
1. http://www.privacyrights.org/ar/ChronDataBreaches.htm
2. Javelin Strategy and Research, annual report 2006
3. Scott and Scott Compliance Simplified 2006
4. PGP Research Report "What does a data breach cost companies. Nov 2005
5. HIPAA Solutions web site February 07, update memo (Acosta v Bryrun) (www.hipaasolutions.org)

The BioSig-ID and Click-ID suite of products are summarized below. For more information about pricing or to ask about a free trial contact Jeff Maynard directly at jeff@biosig-id.com

## Products Summary

**BioSig-ID Online™** – Allows only registered users who have authenticated their identity access to Internet accounts, web sites, and personal data files through any portal. 4 layer, multi-factor identity authentication using gestures captured from your mouse or any pointing device. Enrollment profiles are kept in secure database and used to compare to new signatures/gestures. If the signature falls within certain metrics access is granted. Provides best security in market without the need for any special equipment or hardware. Audit trail log creates compliance 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.

**BioSig-ID WinLogon™ -** As above but application is for the desktop and effectively secures the user from un-authorized access as users must authenticate themselves before logon to Windows.

**Click-ID Online™ -** Provides identity verification using images that are chosen from list or images that the users can load. Select specific objects on your favorite image in order to verify user's identity against a stored profile completed during enrollment. Enrollment profiles are kept in a secure database and used to compare to a new selected image and objects. If the selections are correct, access is granted. 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 WinLogon™-** As above but application is for the desktop and effectively secures the user from un-authorized access as users must authenticate themselves before logon to Windows.

**Click-ID Reset™-** Is a replacement for knowledge based questions or other password reset methods that are browser based. Ideally for single password resets versus multiple application

passwords Creates hardest non-biometric identity verification with simple clicks of the mouse on an image.

**Sig-ID Online™ -** Provides a representation of the signature made by a client using a pointing device such as a mouse. Demonstrates “intent” by a user for verification and evidence of ownership with chargebacks, credit card purchases, online contracts or other electronic purchases especially when used with other personal identifiers.