WELCOME TO THE GEMINI IBD INFOGRAPHICS NEWSLETTER

[VOLUME 1] 03-28-2017

DEBUNKING THE MYTHS OF BIOMETRICS

INTRODUCTION TO BIOMETRICS

Biometrics is a technological tool which can 100% confirm your identity based upon your unique physiological or behavioral traits.

Our Uniquely Human Traits

- The ridges, valleys, and whorls in our fingerprint
- The structure of our face
- The shape of our hand
- The way we inflect our voice when we talk
- The orientation of the tissue groups in our iris
- The pattern of blood vessels which make up the retina
- The way we sign our name
- The typing strokes and patterns on a computer keyboard
- The vein pattern on the back of our hand

When compared to the other security tools and technologies which are out there, Biometrics will be dominating the forefront in the coming years to come. In fact, it is expected to the premier security tool of choice by CIOs in the coming years. Just consider some of these statistics:

2017

+472 Million
Smartphones
Will Use Biometrics
+$10 Billion is the Market Value
of Multifactor Authentication
through Biometrics

2019

+770 Million
Biometrics Apps
Downloaded Annually
+Capital for Biometric
Smartphone Industry
Hits $400 Million
+40% Growth in
Smartphones Using
Biometrics

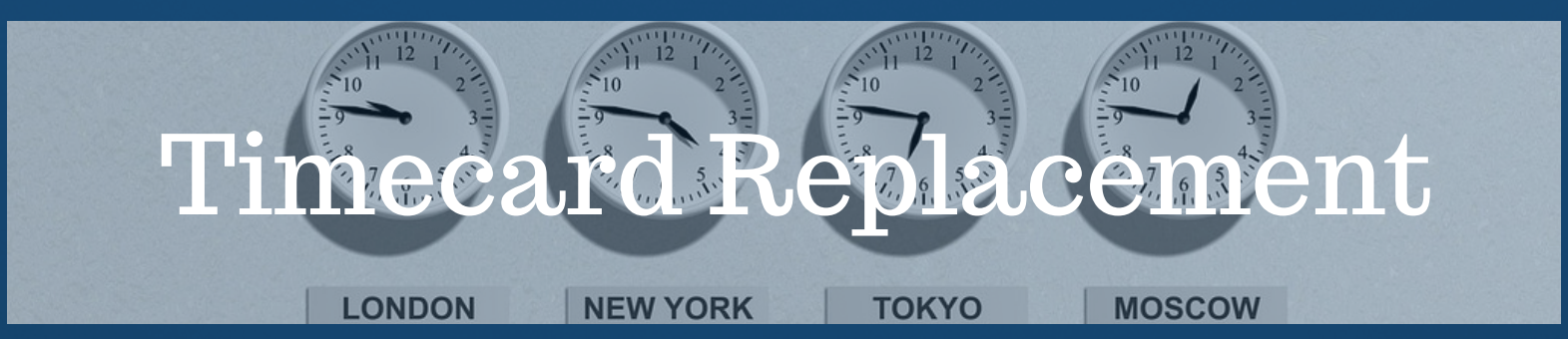
2020

+18% Growth
in Biometrics Market
+$25 Billion Capital
in Biometrics Market
+130% Increase in
Smartphone Biometric
Industry

2022

+$35 Billion Capital
in Biometrics Market
Due to Industry Growth

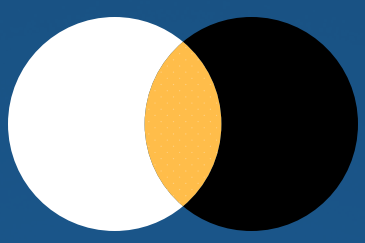
Biometric Applications



Physical Biometrics

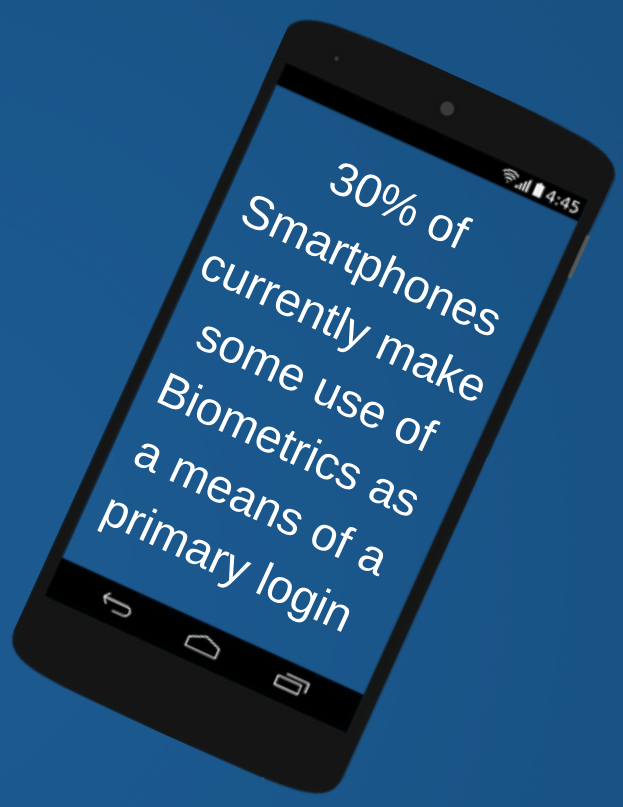
Behavioral Biometrics

Keystrokes

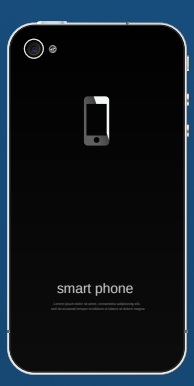


Signature

The North American region (United States and Canada) will hold a 40% market share of the Biometrics industry.



The Asian Pacific countries are the fastest adopters of Biometrics, with a rate of 24% per year and a market capitalization of $3.3 Billion.



The rapid advancements in Smartphone Technology is also driving up the demand for Biometrics.

It is expected that Iris Recognition will be the most popular Biometric Technology, achieving an annual compound growth rate of 26%.

The use of Fingerprint, Iris or Vein Pattern Recognition will see a 27% increase of usage in terms of deployments on Point of Sale (POS) Terminals.

WELCOME

The hospitality industry is expected to make one of the largest uses of Biometrics, with an adoption rate of almost 27%.

Upcoming Technologies

DNA

Ear Lobes

Gait

APPLYING BIOMETRICS

- Passwords are the first choice of attack by Cyberhackers
- It can cost a business up to $300 per year per employee just to reset one password
- With Biometrics, your fingerprint or your eye becomes your password
- With one scan or one swipe, you can be logged into your computer or wireless device in less than 2 seconds
- As a result, your new password cannot be lost, forged, stolen, or hijacked because it literally belongs to you!

We have hundreds of passwords to use. They are often long, complex, and too difficult to remember. As a result, we have to write them down on Post-it-Notes, creating the “Post-It Syndrome”;

Many smaller businesses still use the timecard to keep track of the punch in and punch out times of the shifts the employees work. This is then entered manually into a spreadsheet to compute payroll, which is very laborious, time consuming, and costly.

By using a timecard, there is also the problem when an employee punches in and out the timecard of another employee when he or she is not present at the workplace. This is known as “Buddy Punching”.

- Over 75% of businesses lose money from buddy punching.
- 4.5 hours of productivity is lost per week (equating to 6 weeks of paid vacation in one year).
- Buddy punching accounts for 2.2% of gross payrolls.
- With Biometrics, your hand or your finger becomes your time card.
- An employee can clock in and clock out in just a matter of 2 seconds or less.
- Payroll can be computed in just a matter of minutes, eliminating all of the administrative overhead.
- It also eliminates the problem of buddy punching.

WORLD TRAVEL

Biometric E-Passport

For many decades, the traditional paper passport has been utilized as the de facto standard for confirming the identity of an individual as he or she entered into foreign borders.

But, this paper passport has caused many problems in the past, from a security standpoint. For example, it can be easily lost, stolen, and very easily replicated. Also, if a country does not have an adequate passport processing infrastructure, a foreign traveler could potentially have to wait for hours before being allowed entry into the country of .

As a result, the next generation of passports known as the “Biometric Passport” or “e-Passport” was created. This looks just like the traditional paper passport, but the primary difference is that it has a memory chip inside of it. This chip can contain literally megabytes of information about the traveler, including their Biometric data, such as Fingerprint, Iris, and Facial Recognition templates.

The “e-Passport” also contains a very small, Radio Frequency Identification (RFID) antennae. So, when the foreign traveler enters the immigration line into the country of destination, he or she merely has to ‘flash’ their “e-Passport” in front of the reader. If the Biometric information matches, the individual will be granted entry.

The primary advantages of the “e-Passport” is that a foreign traveler can be processed in just a matter of a few seconds, and his or her identity can be 100% confirmed, unlike the traditional paper passport.

Are you interested in learning more about the “e-Passport”? Read our book: “Adopting Biometric Technologies: Challenges and Solutions”

Top 5 Biometric Myths

1

Did the James Bond Movies inspire the development of Biometric Technology?
No! The James Bond movies did not start the growth of Biometrics. This science and technology has been around for a very long time, starting with the fingerprint and hand geometry recognition scanners dating all the way back to the 1960’s.

2

When my eye or finger gets scanned (or the way I type on a computer keyboard or sign my name), is it the actual image of it which is stored and used to confirm my identity?
When you first register to any kind of Biometric system, yes the actual physiological image or behavioral trait is used to create what is known as the Biometric Template. But typically, this raw image gets converted into a mathematical file, which is subsequently stored and used to confirm your identity. Actual images are never really stored in Biometric systems.

3

Can I get a disease from contact with a Biometric system?
Pretty much all Biometric systems require some sort of direct, physical contact with it. But there have been no known cases in which somebody has actually contracted a serious illness from direct contact with a Biometric scanner. There is a trend now occurring in which some Biometric systems do not require direct contact. The best known examples of this are Vein Pattern Recognition and Iris Recognition. But, there is now a movement in the Biometrics Industry to start developing non-contactless technology, such as that of Vein Pattern Recognition.

4

If my Biometric Template gets stolen, will identity be stolen? Is it the same as credit card theft?
In an absolute sense, yes, it can be considered ID Theft. But think about it. A Biometric template is just a mathematical file. If somebody were to steal it, what can they do with it? Each vendor has their own proprietary systems, so you cannot steal one template and expect to use it another, different Biometric system. And no, it is not the same as credit card theft. You have a much greater chance of somebody trying to “clone” your identity with your credit card number than your Biometric template.

5

Can you take out the eyeball from a dead body and use that at a scanner at a local ATM Machine?
No, this is not possible. Nearly all Biometric systems require a live scan sample. Meaning, you have to be a living person, with a discernible heartbeat in order to be registered into a Biometric system.

Sources

Marketsandmarkets.com

Homelandsecuritynewswire.com

Technnavio.com

Afcea.org

Tensor.co.uk

Securityintelligence.com

Linkedin.com

Blog.m2sys.com

Planetbiometrics.com

Blog.hoyoslabs.com

Findbiometrics.com

Blog.thewfcgroup.com

Usa.visa.com