

# BIOMETRICS — FACT AND FICTION



**Due to the fact that this technology is new to many in the marketplace, it is understandable that there are some misconceptions regarding fingerprint biometrics.**

By Greg Stevens, Account Manager and Kelly Shoemaker, Vice President of Sales & Marketing  
US Biometrics

## Introduction

When new technology is used in a way where it is designed and packaged to solve specific business problems, a new wave of employee productivity, customer satisfaction and cost savings are usually the result. Using fingerprint biometrics properly in corporate America CAN make those goals reality and provide many, many benefits including the following:

- Convenience
- Enforceable Accountability
- Enhanced Logical And Physical Asset Control
- Multifactor Authentication
- Increased Accuracy
- Reduced Liability
- Improved Safety
- Customer Confidence
- Security
- Reduced Internal Costs: e.g., fewer password related help desk calls, key/lock replacement
- Deter and Prevent Fraud and Identity Theft

The purpose of this document is to lay out some very pertinent facts concerning costs, acceptability, and deployment issues so decision makers can make educated and well founded decisions on whether or not to utilize biometrics for solving some, or all, of their identification and authentication problems in the workplace.

Although these benefits sound like the utopia that most companies want to get to — there is a hitch. That hurdle is to be able to logically weed through the misconceptions and misinformation that is always associated with the use of new technologies and then understand its true benefits and shortcomings. Fingerprint biometrics is no different and since its use and acceptability is escalating quickly in the financial, medical, and educational sectors of the world economy, many companies have begun that process of investigating, budgeting, and implementing.

The purpose of this document is to lay out some very pertinent facts concerning costs, acceptability, and deployment issues so decision makers can make educated and well founded decisions on whether or not to utilize biometrics for solving some, or all, of their identification and authentication problems in the workplace. Also, at the very end of the document, specific statistics have been listed that may give some additional insight.

Companies can address numerous multifactor authentication needs by biometrically controlling networks, computers, password change requirements, customer identification and physical access.

### Misconceptions about Fingerprint Biometrics:

Due to the fact that this technology is new to many in the marketplace, it is understandable that there are some misconceptions regarding fingerprint biometrics. The following paragraphs illustrate some of the most common misconceptions followed up by facts about each specific topic.

#### **“Fingerprint Biometric Solutions are Costly”**

Perhaps the largest misconception out there today regarding biometrics is that the systems and solutions are too expensive for the average institution to afford. Nothing could be further from the truth. The majority of the early biometric implementations have been related to governmental spending. As a result, these contracts have been large projects that have not, for the most part, been subject to the forces of a commercial market. Biometric solutions for commercial use are much more competitively priced. As an example, the return on investment (ROI) for a fingerprint biometric solution that

eliminates pins and passwords generally takes less than six to eight months. When purchased with a central repository for fingerprint profile information and extending to identify and protect customers (i.e. Diebold’s identiCenter™ system), the costs can be reduced even more because of the reduction of external fraud. As a firm decides to change core applications, add other software applications, or implement more than one biometric solution, there is no need to pay for a stand alone product for each problem to be solved. The new product is simply added on to the central database server framework which saves both time and money for the institution. An added benefit to this methodology is the fact that since the institution already has the fingerprint profiles enrolled, there is no need to re-enroll employees or customers for the next solution. This increases productivity on all fronts.

#### **“All Biometrics Require a Difficult and Lengthy Integration”**

When most people envision the rollout of a new and revolutionary technology such as biometrics, they often assume that a difficult and costly integration will be necessary to bring the technology to their institution. If a company chooses the correct vendor, this position is incorrect. As an example, US Biometrics’ and Diebold’s identiCenter™ products function by putting a biometric front end via a template onto your Windows™ user accounts or core banking or credit union applications. The result of this method of “integration” is that you are able to achieve biometric authentication and verification in minutes or hours versus weeks and months. A simple evaluation will answer whether or not the technology will work in specific corporate environments and with specific websites, networks, and/or applications. This saves the end user both the money that an integration project requires and the time it would take to make such an implementation successful. Again, time for deployment is days — not months.

#### **“What is the General Public’s Acceptance Level?”**

When examining whether or not to purchase a biometric solution, the company may carry the misconception that they may experience some difficulty in getting the average consumer or employee to accept the technology. In fact, most of the evidence available is really to the contrary when the biometric system is being offered by a trusted source.

"Recently a study was conducted by the BioMarket Project (Jamison Consulting) to assess acceptance of biometrics by the public and IT professionals, it was revealed that over 80% of the public would allow some aspect of their biometric identity to be recorded. The BioMarket Project study also found that the majority of people believe government and industry should be encouraged to use biometric techniques to improve security. Most people would also prefer to use biometrics to access banking and brokerage and credit card services instead of using passwords/pin numbers. The study also specifically listed fingerprint biometrics as the most accepted method due to current public awareness."

An additional study conducted by the Department of Justice via the Bureau of Justice Statistics found that:

"A majority (56% – 91%) of the U.S. public believes it is acceptable for the private sector to use biometric technologies."

In the day and age of identity theft and fraud, the general public knows that they are vulnerable and looks to biometrics as one of the methods viable to keep both their identity and financial information safe and secure.

### **"Is there a Sanitation Issue with Fingerprint Biometric Scanners?"**

Many are concerned about coming into contact with harmful bacteria and germs. It follows that some individuals will have concerns about the cleanliness of a device that may potentially read thousands of fingerprints a day. The good news is that most biometric readers used commercially today can be cleaned relatively easily. A simple combination of solution and wiping can effectively disinfect a reader and cut down

on any excess bacteria that may build up. Companies simply make routine cleaning a part of their maintenance program.

Recently, Purdue University conducted a study to determine the cleanliness of biometric devices at their Purdue's Biometric Standards, Performance and Assurance Laboratory. The study found that:

"While the platen glass surfaces of devices that scan fingerprints or hand geometry may look more unsanitary due to visible dirt and prints, they in fact harbor about the same amount of bacteria as a typical doorknob."

In addition to this official finding, researcher Christine R. Blomeke was quoted as saying:

"Since there is the perception that these devices may cause illness, our study is important in that it at least establishes that a person is not any more likely to become ill from a biometric device than from a plain, old-fashioned doorknob."

## **Conclusion**

As the incidence and frequency of identity theft and internal fraud continue to rise, the financial and medical business sectors look increasingly to biometrics to help them more effectively battle the aforementioned issues. There is the call from the general public for more biometric authentication and verification in trusted environments, but there still exists some misconceptions as to the sanitation, cost, integration effort, and public acceptance that are prohibiting companies from moving forward with a biometric plan. Hopefully, this document sheds some light on the reality of what biometrics can do to bring customer convenience, security, and profitability to its adopters.

Headquartered in Naperville, Illinois and founded in 1997, US Biometrics designs and deploys a wide range of biometric technologies for corporate, financial, governmental, healthcare and educational clients who require absolute authentication of customers and employees.

Contact Information:  
US Biometrics Corporation  
www.usbiometrics.com  
630.922.8200

© Diebold, Incorporated, 2008. All rights reserved.  
05.08



# MISCELLANEOUS STATISTICS AND INFORMATION

## Password Change Impact

Aberdeen's research finds that labor costs for configuring and maintaining password systems for a small company of 100 users averages \$100 – \$150 per user, per year. That equates to \$15,000 in general and administrative (G&A) expenses just to maintain passwords. A mid-tier company of 1,000 users averages about \$200 per user or \$200,000 per year. Finally, a large enterprise with over 100,000 users will experience \$300 – \$350 per user. (*Passwords Are Gobbling Up Your Profits*. Jim Hurley, Aberdeen Group. May 1, 2003.)

EMA research has shown that, on average, password management costs \$250 per year for every technology user in an organization. (*Citrix MetaFrame Password Manager*. Enterprise Management Associates. September 2003.)

In a non-automated support model, password reset costs range from \$51 (best case) to \$147 (worst case) for the labor alone. Password reset represents a call volume range of 10% to 30% at the IT service desk. A typical internal user is required to maintain eight unique user IDs and associated passwords. The cost per user per year for pin and password resets is \$300. (*Password Reset: Self-Service That You Will Love* (Gartner Research Note T-15-6454) Gartner Group, Roberta J. Witty & Kris Brittain. April 15, 2002.)

## Check Fraud Statistics:

- Recent Secret Service investigations indicate that there has been an increase in counterfeiting of corporate checks and other negotiable instruments created with the use of computer technology. (U.S. Secret Service)

- The chief of the U.S. Secret Service financial crimes division calls check fraud "the number one way criminals today are attacking our financial systems." (U.S. Secret Service)
- Losses from check fraud are expected to grow by 2.5 percent annually in the coming years. (*American Banker* magazine)

## Internal Fraud Statistics: (BAI research)

- \$652 billion in revenues are lost annually to fraud, or 5% of total revenues.
- The average fraud scheme lasted 18 months before it was detected.
- Organizations lose 20% of every dollar earned to some type of workplace fraud.
- Fraud reduces net income dollar for dollar, meaning that if the profit margin is 10%, an additional \$100,000 of revenue would have to be generated to cover a \$10,000 fraud.

## Expected Financial Risk for Publicly Disclosed Data:

(IT Policy Compliance Group. *"Why Compliance Pays – Reputations and Revenues at Risk,"* 2007.)

The expected financial risk for publicly disclosed data loss and theft include:

- An 8 percent decline in the market value of a share of stock for publicly traded firms
- An 8 percent loss of customers
- A temporary decline in revenue of 8 percent
- Additional costs for litigation, notification, settlements, cleanup, restoration, and improvements averaging \$100 per lost customer

Headquartered in Naperville, Illinois and founded in 1997, US Biometrics designs and deploys a wide range of biometric technologies for corporate, financial, governmental, healthcare and educational clients who require absolute authentication of customers and employees.

Contact Information:  
US Biometrics Corporation  
www.usbiometrics.com  
630.922.8200

© Diebold, Incorporated, 2008. All rights reserved.  
05.08

