Misconceptions about Biometrics
(In general … and specifically to fingerprint technology)

We live in a paradox. Emerging technologies continue to advance that will dramatically transform and improve our lives. Yet, many, if not most, people tend to resist change. Why? They believe that new technologies are either too expensive, too difficult to set up and use, not necessary, or simply fear upsetting the status quo with something that will not work as well.

Products have a learning curve and are frequently more difficult to use when first introduced. It takes time for general familiarity to increase and user feedback to be reflected in product improvements. Rumors from naysayers who spread pessimistic accounts about past experiences are also a factor. A bad reputation is difficult to erase even after corrections have been made.

What is easy to overlook are shortcomings and risks associated with current solutions that will be superseded and replaced. New technologies offer services and benefits not previously possible in addition to improvements upon a status quo.

All of these have applied to biometrics. Now, after several generations, biometric products have gotten better and better. More and more people are finding value from them while frustrations build with other less effective and outdated solutions. As needs keep growing, changes will continue to accelerate as new and improved biometrics keep coming to market. Getting under the covers to see their real value may take effort, but the rewards will exceed expectations while providing a competitive edge. What is important to realize is that it takes carefully planning and a gradual introduction to avoid becoming overwhelmed and simply replacing one set of problems with another.

Are biometrics "ready for prime time?"

The answer is an emphatic "yes!" Those that consider biometrics with an open mind will find that past excuses are no longer relevant as significant technical advancements have greatly increased business value over initial offerings. Consumers and organizations everywhere can now successfully adopt biometrics for a broad, ever-expanding, range of everyday applications. We expect adoption to accelerate as standalone, once-proprietary solutions (which in actuality were simply components and incomplete solutions) become integrated with each other, allowing them to share matching databases and facilitate a new round of business automation.

What are biometrics anyway?

The word "biometrics" itself can be confusing. Some people think that the term refers to something medical. Actually, ***biometrics*** are a collection of technologies that use unique features and characteristics of individual human beings, including fingerprints, retinas, irises, hands, voices, faces and voices, for identification and authentication purposes. They represent lifetime God-given features of individuals that cannot be readily forgotten, lost, shared, stolen or forged like passwords and other competing authentication products that merely assume someone's identity.

Can anything be more secure than tying identities to actual individuals?

No! In this faceless, global cyber world, which has changed our entire existence on earth, the only way we can put a face on digital identities is to make sure that there is a correlation to one or more unique human features. One identifier, commonly a fingerprint, is usually enough, but some prefer to err on the safe side and add a second biometric such as a retinal scan. Nothing besides biometrics establishes a "foundation of trust" that assures substantiation of those who we deal with via the Internet and any IP-enabled "faceless" electronic relationship.

"Who is the actual person on the keyboard?"

Until now, we simply did not know for sure when we could not see them! Consequently, without biometrics, we have been forced to assume and accept all faceless digital identities over the Internet based upon weak, outdated, circumstantial user credentials such as passwords, tokens and Smartcards.

Cumbersome and user-frustrating procedures have required Personal Identification Numbers (PIN), dozens of multiple passwords for work and personal access, physical tokens, Smartcards, ID cards, and other user

credentials such as IP addresses, MAC addresses, certificates and more. The problem is, absolutely none of these user credentials can prove the identity of the actual person on the keyboard or a host of other examples.

Can't biometrics be fooled?

Sometimes, but let's put things in perspective; nothing is 100 percent effective or perfect. Passwords and other technologies that are commonly used have a growing list of shortcomings of their own. And, yes, biometrics have, at times, been spoofed (tricked) using fake fingers, talcum powder and other creative means. Some scanners are inherently more susceptible than others, but improvements and fixes have gradually lessened the likelihood that spoofing will be successful. Finally, no one should assume that any technology will be a panacea. Nothing by itself will save them from the need to use common sense. For example, phishing attacks trick users into divulging personal information to others who appear legitimate, but in fact are misrepresenting themselves. This applies whether a biometric or a password or anything else is being used.

Why should I make biometrics a top priority for 2007?

In today's insecure world, biometrics are the best hope for real security and compliance improvements over embedded, inadequate alternatives. Biometrics provide cost savings, added revenues and other advantages not otherwise possible with today's best authentication and verification processes. Furthermore, unlike traditional authentication programs, biometrics are not restricted to computers and cyber networks. Convergence is now bringing the cyber and physical worlds together in a common security architecture linked by Internet Protocol communications.

Visionary organizations will realize that their whole business dynamics and corporate earnings will dramatically improve with the start, integration, and gradual deployment of biometrics throughout their company's applications, products and services. Furthermore, as continued advancements in biometrics become more widespread, cost savings and business value will grow continually and substantially.

Fortunately, organizations that make biometrics a top priority for 2007 will reap powerful advantages that have not been available until recently. Unlike previous experiences by early adopters, those who take action now and learn about powerful opportunities from advances in biometrics no longer should expect negative consequences. Beginning with compelling business cases, firms will have successful experiences when doing things carefully thereby gaining experience and increasing benefits.

I have heard about biometrics projects that failed. What went wrong?

Biometric vendors put products on the market that simply were not ready. Vendors "hyped" incomplete and insufficient so-called solutions in attempts to generate cash flow to help offset expensive development and manufacturing costs. The destructive mindset of "***sell them what we have and do not worry about what they actually need***" was virtually universal throughout the early biometric industry.

Biometric vendors were selfish. Instead of being a problem-solving solution provider, each vendor wanted 100% of each project and was unwilling to work with better, competitive and/or complementary components. This was particularly true in the area of fingerprint scanners. Instead of making fingerprint scanners interoperable with those from competitors, vendors selfishly restricted architectures such that scanning hardware would only work with their own proprietary image capture, "1-to-1" matching algorithms, and applications software.

Decisions to push products into the market before they were ready ultimately hurt the entire industry. Technology that was inconsistent and/or difficult to get to work proved totally unacceptable. In all fairness, many past failures with fingerprint technologies were also the result of poor user implementations as much as from failures of the technology itself. Many implementations failed to address business realities and lacked sufficient user training and support.

Can this still happen?

We believe that it could or will happen if end-users do not seek advice when comparing alternatives and examining pros and cons. We have built part of our business around this need.

What do I need to do to be prepared for biometrics?

Projects do not succeed without adequate preparation, training and support. Users as well as the CFOs who pay the bills become particularly disillusioned when they do not see a clear need for biometrics in the first place. Users are especially frustrated when they must make something work that they do not understand and seems to

be merely replacing one set of problems (e.g., administering passwords) with something that is an even bigger headache because it is new and confusing. Companies that take past lessons to heart and include all of the assistance and support users require will be successful.

Why should passwords (and other user credentials) be phased out?

Passwords can no longer do the job that is required from them. Password cracking tools by the thousands can be found free or low-cost on the Internet. These tools are readily downloadable and are a leading cause of serious privacy and data breaches. Furthermore, both consumers and employees are "swamped" with more and more applications requiring passwords and stronger credentials. There are simply too many of them for anyone to manage and secure adequately. Complexity due to password overload is not only inconvenient, but is not cost effective or beneficial, especially when employees put them on sticky notes and criminals use superior technology to defeat the passwords. All of the things to remember and carry around are sources of constant frustration and confusion.

"Single Sign-On" has been touted as THE solution to eliminate multiple passwords and save employee time and help desk expenses. The problem is, SSO may bring greater convenience and simplicity alright but it multiplies corporate risk. With all the hackers, does it make sense to provide a cyber and/or internal criminal all the keys to the kingdom via a single and easily compromised SSO password?

What is needed is something that is not only convenient, but something that is also better and stronger. People are finding it with biometrics.

Will technology give my business 100% protection and compliance?

No! Technology, including biometrics, is still not a total answer. People are the most important factor in making anything secure. Deliberate or careless behavior can be enough to undo the best that technology offers. Processes and procedures are needed to tie everything together into an optimum mix of resources. Awareness, motivation and training are required to ensure that everyone knows what to do on a regular basis and also to deal with unexpected situations should they arise. Also, if something unexpected does happen (and we all know that it eventually will), it makes sound business to have an automated and irrefutable activity log or electronic recording to facilitate audits and the reconstruction of the events that occurred. We recommend technology that does this automatically, enabling every keystroke, website, database and action to be reproduced and reported in real time. This is essential no matter what authentication technology is employed.

Will multiple layers of authentication protect my business?

Although "two (or more) factor" authentication can increase the confidence that the user who is displaying credentials is likely the person that he/she is supposed to be, authentication of this type still is based upon assumptions and circumstantial evidence.

Basic flaws must be recognized. No single or multiple combination of layered authentication (even including traditional "1-to-1" biometrics that does not prevent the use of aliases) can possibly prove 100% (beyond the shadow of a doubt) who a faceless person really is. The best identification requires alias-free, "1-to-many biometrics. Anything less increases risk but may be adequate based on tradeoffs.

With Internet usage expected to double to 2 billion people by 2010, the escalating possibility of fraud regarding e-commerce and e-banking is too serious to leave to chance. Furthermore, as institutions require customers to also use physical tokens, Smartcards, and other added forms of authentication, mistakes and lost credentials will increase costs and inconvenience and defeat the value of added protection.

Besides being inadequate to address heightened risk in today's global cyber infrastructure, similar issues apply to technologies that have been used to secure our physical world. Solutions that are unnecessarily complicated, time consuming, inconvenient and expensive to deploy, manage, and reissue when devices are stolen, lost and forgotten, must be replaced. As physical and cyber worlds converge, biometrics will play a greater role in controlling access to physical, as well as cyber, assets.

Are all fingerprint biometrics equal in application and performance?

No! Fingerprint scanners (readers) were originally installed in a variety of different computer-related devices (standalone, mouse, keyboard, and laptop). They are now being introduced into an increasing variety of custom applications and hardware including turnstiles and gates.

The active elements (chips) used in scanners come in different sizes and shapes and use different technologies (i.e. optical, capacitive, electro-luminescent, pressure, MEMS, RFID, silicon swipe, and others). What is not so obvious is that scanners differ in durability, reliability, accuracy, speed, consistency, usability and value. Relative value, however, may or may not be apparent based upon a comparison of prices. Some products may in fact be better from a technical and functional standpoint as well as being cheaper. It is important to reflect varied tradeoffs in the selection process.

Although there have been many advances in scanners, not all fingers work the same with scanners. Even the same individual may have different operating characteristics from finger–to-finger and time-to-time that cause a particular sensor to work better one time than another. Scanners keep getting better. This is why we warn clients that we have yet to find a single fingerprint scanner that will work consistently on 100% of the people, 100% of the time. However, with the proper integration of interoperable components, solutions that provide a choice of scanners are available that will.

The key factor making fingerprint technologies and form-factors user-friendly is taking enough time to educate and execute proper enrollment procedures. For example, if a user's fingers are scanned on multiple scanners, the best image, independent of vendors' technologies, should be used to create the stored templates. Users can then use any other interoperable scanner whenever they logon in the future since they will be comparing against the best possible matching template.

Be forewarned, however. Vendors will try to dissuade you from considering something that is interoperable and has a competitive bias against their products. Some are even successful in getting their chips hardwired to OEM products such as laptops to grab a captive market and not necessarily in the best interests of the user. For your greatest benefit, flexibility and an agnostic viewpoint are essential. Research carefully before committing to any product or technology, especially one that has limited flexibility.

What should be expected in the long-term from biometrics?

In general, expect biometrics to eventually become cheaper and better in every respect. However, this should not discourage anyone from seeking immediate value from today's products. With proper planning and selection, future product improvements should, in large part, seamlessly blend with those already deployed.

Look for improvements in durability, dependability, accuracy, speed, usability, functionality, convenience, ease-of-installation, configuration and use, variety of applications, and integration that allows common resources to be shared. Along with integration, expect automation of standalone applications based upon a broad foundation of trust. Built-in trust facilitated by biometrics will enable and deliver confidence in having unattended machines accurately, reliably, responsibly and honestly handle transactions via integrated processes and procedures. Machines will increase quality and performance without the need for complicated checks and balances to offset human carelessness and fraud. Biometrics will be capable of being used to authorize the start of automatic processes that perform assignments and fulfill duties including the making of self-service retail purchases and payments with built-in, operator-free monitoring, tracking and auditing of results.

How should we get started with biometrics?

START is a key word. Start with baby-steps including conceptual brainstorming, planning and trying out / testing a "short list" of different fingerprint scanners, interoperable image capture software and matching algorithms under actual user operating conditions. This process is relatively "painless" and inexpensive, but the educational value will prove priceless. We encourage starting before something happens, i.e., a breach, that forces implementations to be rushed without adequate preparation and support.

Refining and expanding the process should be done carefully. This is not time-consuming or high-risk, but it will bring increasing value to each and every employee and other users, including customers, as budgets and support resources become available. A "big-picture" perspective that reflects diverse business needs and what it takes to make customers, employees and 3rd party partners happy and cooperative is essential. Involving these important groups of users in the selection and testing process will build goodwill and help to establish a foundation that will enable successful testing, trials and eventually a successful rollout to an entire user base.

If I get started now, will I have to start over when products improve even more?

We would not want to promise that nothing will need to be replaced before its time, but replacements should be kept to a minimum and pay for themselves with cost savings and added revenues in any event before changes

become necessary. Any disruptions will be minimized when the right things are done. This starts with picking products that are interoperable with other vendors' products to minimize sourcing problems as well as to facilitate future customization and integration.

In summary . . . .

There is no doubt that this brief paper does not provide the full complement of insight and expertise that a professional consultation will add to your successful planning and implementations. However, by now, most readers probably have enough to think about.

We encourage you to consider our consulting and advisory assistance to help with everything from brainstorming to a "big-picture" perspective, to suggesting the right products, initial evaluation materials, change management techniques and employee training. Finding the best products can be especially challenging when they are only available from small startup companies.

Our expertise and deployment roadmaps allow clients to envision future enhancements and cover all the bases ensuring success and maximum return on affordable investment capital. We save considerable time and expense cutting through distractions, half-truths and other confusion. We help to make certain that nothing is overlooked that would detract from prompt, growing and continuing benefits associated with a successful enterprise-wide biometric program. We also help clients put together the business cases that justify project expenditures and compare alternatives.

Thank you for your interest. Please contact us.

Tom Rockwood - 973-635-1970
Dave Kern – 508-362-5834

Info@Rockwood.com
www.Rockwood.com