

---

# *Financial Fraud*

BIOMETRICS POINT A FINGER

---

**CELENT**

[www.celent.com](http://www.celent.com)

## Copyright Notice

**Prepared by**

Celent, a division of Oliver Wyman

**Copyright © 2008 Celent, a division of Oliver Wyman.** All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Celent, a division of Oliver Wyman ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. This report is intended to be read and used as a whole and not in parts. Separation or alteration of any section or page from the main body of this report is expressly forbidden and invalidates this report. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification. Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report. No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.

MARCH 2002

**Christine Barry**  
cbarry@celent.com

**Celent Communications**

489 Fifth Avenue  
12th Floor  
New York, NY 10017  
USA

Tel.: +1.212.490.2220  
Fax: +1.212.490.2225  
Email: info@celent.com

www.celent.com

**TABLE OF CONTENTS**

EXECUTIVE SUMMARY .....	3
INTRODUCTION .....	4
MARKET OPPORTUNITY .....	6
SIGNIFICANT OPPORTUNITY .....	6
MARKET SIZE AND POTENTIAL .....	6
GLOBAL ADOPTION .....	7
THE AFTERMATH OF SEPTEMBER 11 .....	8
PRIVACY ISSUES .....	8
TECHNOLOGY .....	10
TECHNOLOGY BREAKDOWN BY SECTOR .....	13
FACIAL RECOGNITION .....	14
FINGER SCANNING .....	14
HAND GEOMETRY .....	15
IRIS RECOGNITION .....	15
SIGNATURE VERIFICATION .....	16
VOICE AUTHENTICATION .....	17
BIOMETRICS AND FINANCIAL SERVICES .....	18
PHASE 1: INTERNAL USE .....	18
PHASE 2: ON-PREMISE CUSTOMER USE .....	19
PHASE 3: REMOTE USE BY CUSTOMERS .....	20
CHOOSING THE RIGHT BIOMETRIC DEVICE .....	22
FUTURE TRENDS .....	25

---

## EXECUTIVE SUMMARY

Identity theft is the fastest growing crime in the United States, affecting more than 700,000 individuals in 2001. In addition, a study completed by the Federal Reserve found that more than 60% of bank fraud cases involved company employees. Financial institutions are therefore at risk both internally and externally. At a time when security fears have reached new heights, it has become increasingly obvious that current security methods, especially passwords, are insufficient and extremely expensive to boot.

Greater security demands are being placed on financial institutions as a result of September 11. The obvious inadequacy of current systems is causing the industry to investigate new technologies to enhance current security methods and replace those most susceptible to fraud. Decreasing costs, higher accuracy levels, and changing consumer attitudes have positioned biometric technologies as a very viable option.

Biometric technologies provide greater security, eliminating the need for passwords. This technology can be divided into seven major sectors: facial recognition, finger scanning, hand geometry, iris recognition, retina scanning, signature verification and voice authentication. While physical and behavioral characteristics are captured in different ways by different devices, almost all biometric technologies work in the same way. They are not all equal however, and specific criteria should be considered before purchasing a device.

Great strides have been made within the biometrics industry over the last few months as the players are forced to emerge from a state of infancy. As they begin to respond to greater attention and demand for their products, we anticipate the following trends will help to reshape the biometric industry in the next couple of years:

- Increased overall acceptance leading to wide-scale deployments, and an expansion in usage as the technology is moved out to the customer.
- The industry will move forward as technologies are created to comply with a new industry standard.
- Consolidation and integration of biometric devices has already begun to occur and is likely to continue.
- Vendors will partner with integrators as an additional distribution channel.

---

## INTRODUCTION

Security is currently a top priority for businesses, government, and consumers. President Bush has allocated more than \$37 billion of the 2003 federal budget to homeland security. Consumer expectations for acceptable levels of security have vastly changed since September 11. In essence, we have experienced a paradigm shift with respect to security, privacy, and intrusiveness, and the balance between them has been altered forever. As a result, providing greater security has become not merely a goal, but a requirement for companies and organizations around the globe.

While financial services fraud pales in comparison to national security matters, security issues touch all aspects of our lives, including our finances. Identity theft is now the fastest growing crime in the United States, and September 11 illustrated to the world its potential ramifications. Security and trust are the lifeblood of a financial institution's existence. Higher expectations and inadequate security systems are causing the industry to investigate new technologies to enhance current systems and to replace those most susceptible to fraud. Consumer fears are also a driving force to change as they place greater demands on their institutions. Increased security is needed and biometric technologies appear to be a viable option.

Biometrics are technologies that identify individuals based on unique physiological and behavioral characteristics. Biometrics provide more robust security than passwords, PINs, smart cards, tokens, or PKI because they identify individuals themselves rather than devices that can be lost or stolen and subsequently placed in the hands of unauthorized users.

Biometric technologies are not new. In fact, most of the major players have been around for quite a few years. Nonetheless, the industry has remained in its infancy. Prior to September 11, usage had been limited to primarily government and law enforcement activities. While financial institutions were concerned about consumer acceptance and privacy, biometric technologies were viewed by many as something out of a science fiction movie. Today, however, with greater attention paid to educating the public and a stronger emphasis on security (even at the expense of privacy), most large financial institutions and card companies have biometric pilots in place. (The few that have fully deployed the technology have done so on a small scale, with most usage to date for internal access to data centers and networks.) In addition, improvements have been made to the technology resulting in smaller devices, higher accuracy, and decreased costs, making it a more attractive and feasible alternative to even small institutions.

This report will discuss the vulnerability of passwords and the need for stronger security measures such as biometrics. It will look at some of the major trends within the biometric

space and how the industry is quickly coming to maturity. It will explain how biometric technology works and analyze the benefits and shortcomings of seven different sectors within the industry: facial recognition, finger scanning, hand geometry, iris recognition, retina scanning, signature verification and voice authentication. It will also describe current usage by the financial services industry, its potential, and criteria to consider when choosing the appropriate devices. Finally, it will conclude with a section on future trends, including a discussion of where we believe the industry is headed in the next one to two years.

---

## MARKET OPPORTUNITY

### SIGNIFICANT OPPORTUNITY

Identity theft is the fastest growing crime in the United States, affecting more than 700,000 individuals last year. A study completed by the Federal Reserve also found that more than 60% of bank fraud cases involved company employees, putting financial institutions at risk both internally and externally. At a time when security is a top concern for everyone, it has become increasingly obvious that current security methods, while extremely expensive, are not sufficient. Passwords, the most widely used security method, are easily forgotten and stolen, and banks spend an average of \$150-200 per user, per year resetting them. Biometric technologies enable financial institutions not only to eliminate costly and inadequate passwords, but also to provide audit trails and to verify individuals without requiring them to carry or memorize information that can easily be lost or forgotten. The identification is the individual himself.

Moreover, in order to control costs and meet customer demands, financial institutions are striving to move more and more of their services to the Internet. The ability to positively verify and authenticate who is actually at the other end of a transaction is a major obstacle preventing financial institutions from moving their most critical and profitable transactions online. Biometric technologies can help them overcome this obstacle by providing a means to ensure, with high certainty, that a remote user is who he or she claims to be. This same level of certainty cannot be achieved with a password.

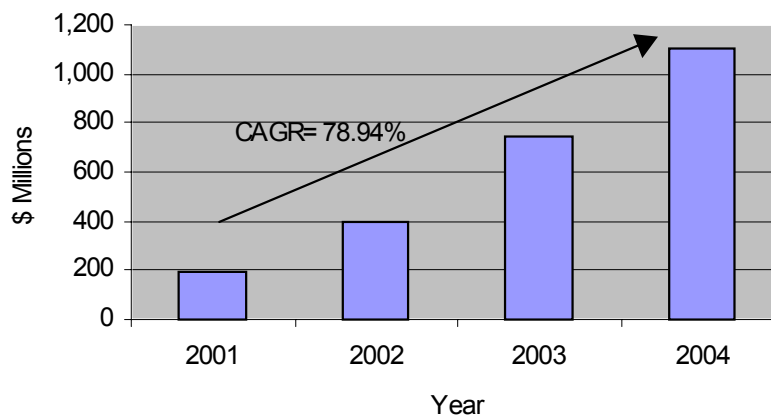
### MARKET SIZE AND POTENTIAL

The events of September 11 have created greater awareness of and demand for biometrics, with pilots being launched in record numbers. In addition to quick deployments at several airports around the globe, financial services and health care institutions have become targets of many biometric developers, who perceive these businesses as good fits for the technology.

The biometrics space is crowded, with more than 200 companies competing for business. This number is likely to decrease as the industry consolidates, leaving behind only those players able to make good on their promises and to provide the greatest return on investment. A few mergers have already taken place, with the most recent, between Identix and Visionics, announced in February 2002. This merger combines two companies specializing in two areas of biometrics, finger scanning and face recognition respectively, to provide integrated and complementary biometric capabilities, a trend that is likely to continue.

The biometrics industry can be broken down into seven major device categories: face recognition, finger scanning, hand geometry, iris recognition, retina scanning, signature verification, and voice authentication. To date, finger scanning has been met with the greatest success in terms of number of deployments as a result of ease of implementation, greater public recognition, and low cost. Usage in general has been primarily for physical access to secure areas. The industry as a whole generated almost \$200 million in revenue last year, with a surge of sales after September 11. This number is expected to grow dramatically as awareness continues to increase and as the population becomes more educated about the technology's benefits. As illustrated in Figure 1, sales are likely to exceed US\$1 billion by the end of 2004.

**Figure 1: Biometric Sales Forecasts**



Source: Celent Communications

## GLOBAL ADOPTION

To date, the majority of biometric vendor revenues have come from physical access deployments. The geographic regions most willing to adopt the technology vary by device type, with the majority of deployments overseas prior to September 11. Since the attacks, the United States, somewhat characterized as having an ingrained mistrust of large organizations, has become more willing to test new security devices, even at the expense of privacy. In Asia, the physical access market is a big area. Japan has been a quick adopter, as has China, which is quickly trying to leapfrog ahead on the technology front after just having been accepted into the WTO. Whereas more developed countries like the United States have the challenge of breaking old habits such as the comfort levels associated with older technologies, countries like China do not have such habits and are very accepting of new technologies. That Europeans have also been fast adopters of various biometric devices is not surprising given their early adoption of mobile banking and smart cards. In the area of finger scanning,

however, the United States appears to be in the lead. This is due, in part, to the role fingerprints already play in our lives. For example, several states now require fingerprint samples in order to be issued a driver's license. In light of these common uses of fingerprints, security-related requests for fingerprints would seem less intrusive than other kinds of biometrics.

## **THE AFTERMATH OF SEPTEMBER 11**

Since September 11, some US industries, such as aviation and trucking, have already been subject to new federal regulations and standards. While the changes in other sectors have not been as formal, the horrific attacks changed the way the world looks at security. Companies in all sectors have begun to review current security methods and systems and are challenged to determine what level of security they will be held responsible for providing.

The common law requires companies to apply the "reasonable man" standard of care. Today's reasonable man however, is not the same man he was prior to September 11. Before the attacks, consumers placed high importance on speed and convenience. They did not want to provide several forms of identification and they wanted as little interaction with others as possible. Companies complied as much as they could with consumer preferences and as a result opened themselves to the potential for fraud.

Since September 11, consumer attitudes have changed. Security and protection of one's identity have become extremely important, even at the expense of privacy. In fact, many now take greater comfort in extra security measures, despite the added inconvenience. Fear is the motivator as many people feel very vulnerable in all aspects of their lives. This focus on security is leading to increased pressure from customers, a driving factor in the large number of security pilot programs now underway. A large percentage of these pilots involve biometric technologies, a technology feared to be too intrusive prior to September 11.

## **PRIVACY ISSUES**

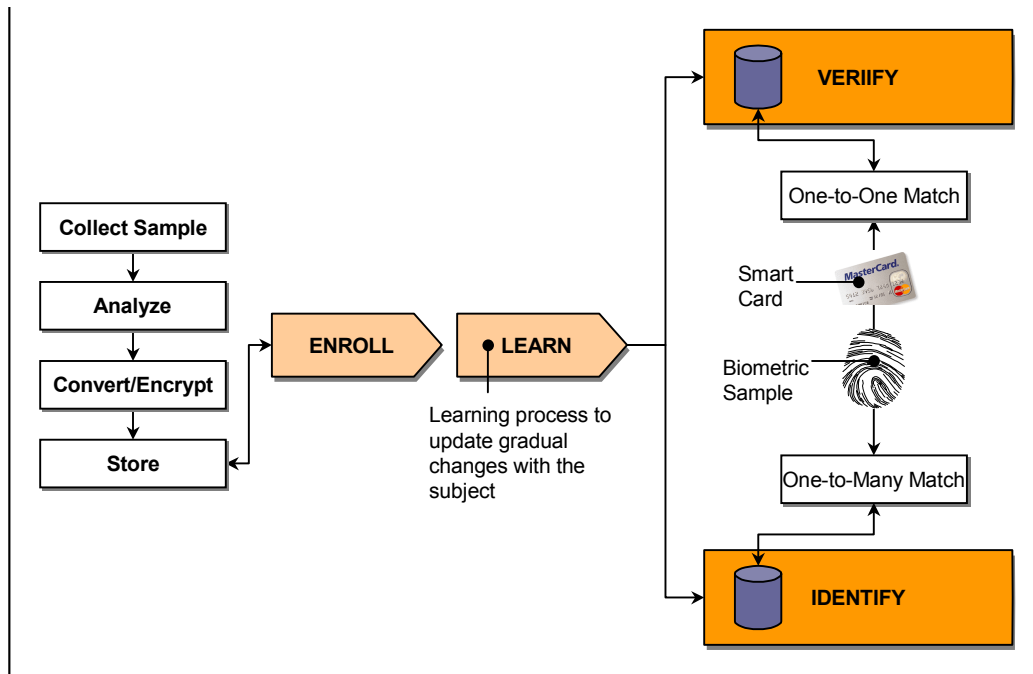
As the public becomes educated on biometric technology and how it works, many will find it is far more secure than one had imagined. In the past, a common misperception was that biometric technologies took pictures of identifying characteristics and stored these images on servers. This was viewed not only as an invasion of privacy but many feared that these images could be compromised or stolen. These fears were not warranted, however, as a finger scanner, for example, does not capture a full image of the user's fingerprint, but instead measures individual "minutiae points"—the distinctive characteristics of an individual fingerprint. The technology then applies a mathematical algorithm to produce a highly unique set of numbers or codes. These codes are stored in the form of a template, not images. The same is true of all other types of biometrics—images are never stored. Moreover, the codes

stored on these templates cannot be reverse-engineered, ensuring that a compromised template is of little value to a potential imposter.

## TECHNOLOGY

While physical and behavioral characteristics are captured in different ways by different devices, almost all biometric technologies work in essentially the same way:

**Figure 2: Biometric Methodology**



Source: Celent Communications

## ENROLLMENT

Before an individual can be identified or verified by a biometric device, they must first complete the enrollment process in order for a template/user profile to be created. Enrollment is typically completed in under two minutes, but consists of several steps:

- **Collect Sample:** The user begins by providing a minimum of two to three biometric samples by, for example, placing their hand on a hand reader for scanning. The quality of the sample, as well as the number of samples provided often influences accuracy, as averages are taken, thereby removing outliers.

- **Analyze Unique Characteristics:** Full images of the biometric sample are not taken or stored. Instead, the technology analyzes and measures various data-points that are unique to each individual. The number of points measured varies by device type.
- **Convert and Encrypt:** The measurements and data-points are then converted into a mathematical code and encrypted. These codes are extremely complex and cannot be reverse-engineered to recreate the original image.
- **Store as Template:** The codes are then stored as a template/user profile in a variety of places including the server of the institution, on a user's PC or PDA device, on a smart card, or in a small number of instances, they can be housed by the licensing developer.

## LEARN

Profiles are often updated each time the individual uses the system through a process called “learning” which takes into account gradual changes due to aging, weight changes, etc. They are later used by the system each time the individual provides a new sample to determine whether access is granted or denied.

## IDENTIFY/VERIFY

Once an individual has been enrolled in a system, they may begin to use the biometric technology to gain access to networks, data centers and buildings, or to access personal account information and authorize transactions. Biometric technologies determine whether or not a person should be granted access in one of two ways: through identification or verification. Most devices have both capabilities and the benefits of each are explained in greater detail in a later section of this report.

- **Identification** is a one-to-many match. The user simply provides a biometric sample and the system searches through its entire database of user profiles to find a match. If a match is found, the user is “identified” and granted access. If no match is found, access is denied.
- **Verification** is a one-to-one match and requires the user to provide identification such as a PIN, smart card, or token, in addition to a biometric sample. In other words, the user is saying “this is who I am” and the system is merely verifying that the claim is correct. The new sample along with the additional identification is then compared to a

previously stored user profile. If a match exists, the individual is “verified” and granted access. If not, access is denied.

## TECHNOLOGY BREAKDOWN BY SECTOR

Biometric devices can be broken down into two groups: physical and behavioral. Face recognition, finger scanning, hand geometry, iris recognition, retina scanning, and voice authentication technologies require analysis of physical aspects of one's body. Behavioral biometrics such as signature recognition, on the other hand, analyze attributes about the way a person moves, such as the speed and pressure they place when signing their name. This section will describe the seven major sectors within biometric technologies and analyze some of their strengths and challenges.

**Table 1: Comparison of Biometric Sector Benefits and Challenges**

Sector	Benefits	Challenges
<b>Facial Recognition</b>	<ul style="list-style-type: none"> <li>- A database of mug shots already exists</li> <li>- Very low level of intrusiveness</li> <li>- Easy implementation as many already have web cameras</li> <li>- Can easily be integrated with other types of biometrics such as iris scanning</li> </ul>	<ul style="list-style-type: none"> <li>- Privacy issues exist as technology can be used without individuals knowledge</li> <li>- Not good fit for environments with poor lighting</li> </ul>
<b>Finger Scanning</b>	<ul style="list-style-type: none"> <li>- Low cost and easy to use</li> <li>- High consumer awareness</li> <li>- Proven track record</li> </ul>	<ul style="list-style-type: none"> <li>- Cannot be used by all individuals</li> <li>- Hardware must be purchased</li> </ul>
<b>Hand Geometry</b>	<ul style="list-style-type: none"> <li>- Easy to use</li> <li>- Easily integrates with other device types</li> <li>- High level of consumer comfort with technology</li> </ul>	<ul style="list-style-type: none"> <li>- Individual measures are not unique</li> <li>- Hardware must be purchased</li> </ul>
<b>Iris Recognition</b>	<ul style="list-style-type: none"> <li>- High accuracy</li> <li>- Several data-points</li> </ul>	<ul style="list-style-type: none"> <li>- Expensive compared to other devices</li> <li>- Perceived to be intrusive</li> <li>- Low public awareness and understanding</li> <li>- Need to purchase hardware</li> </ul>
<b>Retina Scanning</b>	<ul style="list-style-type: none"> <li>- The most accurate of all biometric devices</li> </ul>	<ul style="list-style-type: none"> <li>- Not user friendly and very expensive</li> <li>- High level of intrusiveness</li> <li>- Need to purchase hardware</li> </ul>
<b>Signature Verification</b>	<ul style="list-style-type: none"> <li>- A signature has served as a form of ID for years so not perceived to be intrusive</li> <li>- Easy to use and easily integrates</li> <li>- Eliminates paper, reduces costs</li> <li>- When used with PDA or phone, device is multi-purpose</li> </ul>	<ul style="list-style-type: none"> <li>- An individual's signature changes constantly</li> </ul>
<b>Voice Authentication</b>	<ul style="list-style-type: none"> <li>- No hardware to purchase other than phone or microphone which most have</li> <li>- Easy to use and unobtrusive</li> <li>- Well suited for remote authentication</li> <li>- No need to disclose personal information</li> </ul>	<ul style="list-style-type: none"> <li>- Perceived to be less accurate</li> <li>- Must be able to identify individual using different channels- landline versus mobile</li> </ul>

Source: Celent Communications

## FACIAL RECOGNITION

Traditional facial recognition technologies identify individuals through a number of measurements and physical characteristics such as the distance between one's eyes, the structure of the nose, and the corners of one's mouth. User samples are captured by looking into a camera and depending on the developer, data is captured from either a single or multiple angles. This technology identifies an individual similar to the way the human brain helps us to recognize each other and pick someone out of a crowd.

Advances in facial recognition technology have enabled greater accuracy through learning capabilities that not only enable the system to recognize individuals as their faces go through gradual changes, but which can also recognize them in different light settings at different angles. One of the technology's greatest assets is also one of its largest drawbacks: because facial recognition is perhaps one of the least intrusive of all biometric devices (it requires no more than standing in front of a camera), it therefore can be used without one's knowledge or consent. Such was the case during the 2001 SuperBowl when the technology was used to scan the crowd for individuals with criminal records. This usage without consent resulted in protests from privacy advocates.

Facial recognition technologies are a good fit for physical and network access as well as for ATM security, where cameras are already in place.

## FINGER SCANNING

Finger scanning is the most widely deployed biometric technology as a result of its low cost, ease of use, and high profile. It is also the most competitive space in terms of vendors, as there are between 50 and 75 developers of finger-scanning technology. The technology identifies an individual by the many ridges and bifurcations, known as *minutiae*, that comprise one's fingerprint. A major challenge faced by developers in this space is achieving sufficient measurement detail and resolution from an area that is quite small, as well as one which is easily affected by the wear and tear of daily life. Individuals who work with their hands, such as carpenters, often cannot use this technology as many of the measurements cannot be captured.

Finger-scanning technology can be broken down into three categories: optical, silicon, and ultrasound. Optical scanning has existed for the longest time and is the most widely used of the three, but there appears to be a trend toward silicon. Silicon generally produces a better image quality, and the chips are small enough to be integrated into many devices which cannot accommodate the larger optical technology. Ultrasound, the least widely used of the three, is capable of penetrating dirt and residue on the platen and the finger, countering a main drawback to optical scanning.

It is important to note that this technology is different from traditional ink fingerprints in that it looks at minutiae points as opposed to the entire fingerprint image.

## **H A N D   G E O M E T R Y**

Hand geometry authenticates an individual's identity by the geometric shape of their hand. An individual typically uses the device by placing a hand on a hand reader. As opposed to fingerprints, which are all unique, individual measures of the hand, such as finger length and curvature, are not unique, and only enable verification of one's identity when combined. Because of the lack of uniqueness, this technology produces the best results when used for verification as opposed to identification. Scanners do not measure fingerprints, lines, scars, or fingernails, which may change length from day to day, but do automatically adjust for gradual changes due to aging, or weight changes. Currently one vendor, Advanced Biometrics, circumvents the lack of uniqueness of one's individual hand measurements by taking subcutaneous biometric measurements of the palm instead. In this way, the technology uses proprietary algorithms, photo-optics, and infrared lighting to positively identify individuals through the unique pattern of blood vessels and tissues inside the palm of the hand.

To date, hand geometry technology has been used primarily for physical access environments and works well when integrated with other types of biometrics such as finger scanning.

## **I R I S   R E C O G N I T I O N**

Iris recognition leverages the unique features of the human iris and is one of the most accurate of the biometric technologies. It is based on visible qualities of the iris, such as the rings, furrows, freckles and the corona, which are then converted into a 512-byte template that is stored for future verification attempts. The quantity of the information derived from the iris is said to have 266 unique "spots" or datapoints compared to 13-60 for traditional biometric technologies.

This technology is used in conjunction with cameras that take snapshots of different spots of the iris. The distance the user must stand from the camera differs by camera. Usage involves no touching and the camera differs from traditional cameras in that there are no flashes. There is also no need for light to be flashed at the eye in this type of technology, a major complaint about retina scanning technology.

In its early days, iris-recognition technology was fairly cumbersome and expensive. Recent technological breakthroughs, however, have reduced both the size and price of the devices. While it is still one of the more expensive biometric technologies, prices have fallen to approximately \$240 for the hardware and software. This cost varies, however, based on application and volume.

## Retina Scans

Retina scans are the most accurate biometric technology, but also the slowest to be adopted, perhaps because of its high price and perceived high level of intrusiveness. There is currently only one vendor in the space, EyeDentify, with one product, the Icam 2001. The device weighs approximately two pounds and although it is small enough to be used as a desktop unit, the nature of the device lends itself to wall-mounted implementations. It is the most expensive of the biometric devices, costing approximately \$2,000 to \$2,500 per device depending on the quantity purchased. Perhaps the greatest concern about retina scanning is the use of a light shined into the user's eye. This is necessary because the device must be able to read the capillaries on the retina, which is located in the back of the eye. While the Icam 2001 is also not very user-friendly, it is not intended for retail or home applications where ergonomics and ease of use are essential criteria for deciding on a biometric technology. It is best utilized for physical access to secure locations.

## SIGNATURE VERIFICATION

Handwritten signature verification verifies an individual's identity by measuring the manner in which the user signs his or her name, password, or pass-phrase. It does so by analyzing characteristics such as stroke order (e.g., did the "t" get crossed from right to left and did the "l" get dotted at the very end), speed of hand movement, pressure of writing instrument, etc. These unique dynamics derived from a person's muscular dexterity are usually referred to as "muscle memory" and are automatically controlled by the brain. It is a difficult biometric to track because unlike most other types, the measurements are not static; a person's signature changes all the time and an individual never signs exactly the same way twice. The technology therefore works by tracking gradual changes and recognizing consistency.

In July 2000, former President Clinton signed the e-signature legislation making secure electronic signatures as valid as handwritten signatures on paper. This was a big step for the signature verification space. Since that time, this biometric has enjoyed increasing demand from companies looking to securely close transactions online by binding them with a signature and from those looking to develop a non-repudiated document trail. The signer's identity is not only verified, but fraud is also prevented, as changes to documents cannot be authorized without obtaining another signature. An added benefit and driver for some companies is the cost-saving associated with eliminating paper. It is believed that 15% of corporate revenue can be saved in this way.

An individual uses signature verification by signing their name on either a digital tablet or directly onto a PDA or smart phone. The technology is already being used to a small degree in mobile banking through the use of a PDA, in branches to open new accounts while at the same time maintaining electronic records, and to simply gain access to devices such as PDAs.

The technology is also a good fit for point of sale credit card payments where the user is already signing their name.

## **VOICE AUTHENTICATION**

Voice authentication identifies individuals through measures of both physical characteristics such as length of vocal chords and behavioral characteristics. It differs from voice recognition in that it confirms a speaker's identity by creating and matching a voiceprint, rather than just telling you what is being said. Some vendors, such as Nuance, offer products with both capabilities. In contrast with most biometric devices that work well in physical access environments, voice authentication technology fits best with mobile and remote access verification. For example, it enables customers to access their accounts and perform transactions over the telephone by simply speaking a chosen phrase or random set of numbers as opposed to providing a pass-code or phrase, such as a PIN or mother's maiden name, that can easily be stolen or used by an unauthorized individual. Voice authentication technologies can shorten the identification process to a matter of seconds, resulting in cost savings to the institution.

An individual uses voice authentication technology by calling an institution's telephone banking number. Then, depending on the system, they are asked to provide some type of speech, by repeating a requested set of random digits or by saying a pre-approved code or phrase. The system then calculates a score based on matching specific measures and comparing them to a saved voiceprint. The strength of the match determines whether access to the system is denied or approved.

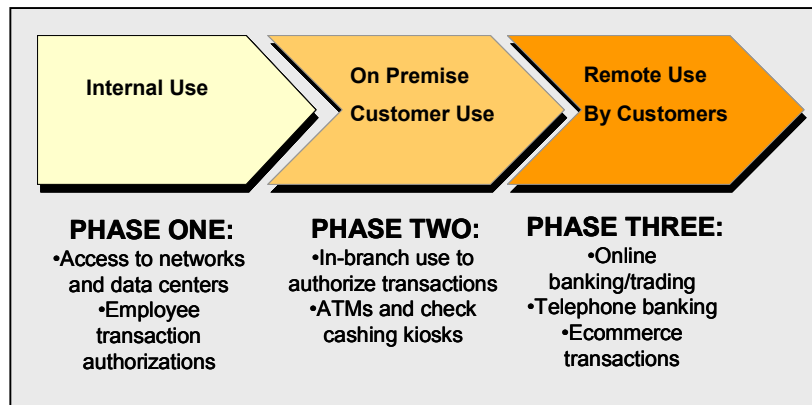
Voice authentication often works in conjunction with a speech recognition system enabling the user to complete transactions without ever speaking with a live person. Every user, however, always has the option at any point to be connected with a live agent. While voice recognition technologies have at times been criticized for their accuracy levels, voice authentication technologies are able to achieve accuracy levels above 99%. The hurdle for this sector has been overcoming the challenge of identifying individuals across multiple channels such as land lines and mobile phones.

Demand for voice authentication is likely to grow as financial services customers become more mobile. To date, the technology has met with the greatest success in the United States, the United Kingdom, and Japan. It can be used to reset passwords, as a call center gateway, for remote telephone access, and for Web banking/trading (through use of a computer microphone).

## BIOMETRICS AND FINANCIAL SERVICES

Adoption of biometric technologies within the financial services industry appears to be following an evolutionary process as illustrated in Figure 2:

**Figure 3: Three Phases of Biometric Technology's Evolution**



Source: Celent Communications

### PHASE 1: INTERNAL USE

To date, most deployments and pilot programs are using biometric technologies internally for employee access to physical data centers and to prove one's identity when logging onto networks and accessing secure information. It has also been used to authorize transactions and to establish an audit trail linking users to transactions. On Wall Street, many brokerage houses have begun investigating systems that allow companies to verify the identity of stock traders before executing large trades. Internal use makes sense during Phase 1 because institutions must first become comfortable with the technology themselves before making it available to their customers.

The following are examples of financial institutions that have announced Phase 1 deployments:

- Indonesia's **Bank of Central Asia** placed a US\$400,000 order for 500 Identix finger scanning units to be deployed in select branches throughout Indonesia to be used internally to securely process high-value electronic fund transfers. These systems are in addition to more than 3,000 Identix systems already in place for the same purpose within the bank. Bank tellers and managers are enrolled in the system

and assigned specific levels of approval for these transfers and an audit trail is maintained.

- **Bank of Brussels** is currently securing access to its data centers with iris recognition technology.
- **California Commerce Bank** improved employee productivity by replacing multiple passwords with finger scanning technology to access its networks.
- Almost all major financial institutions are now at least piloting some type of biometric technology for internal use. Many of the implementations, however, have remained confidential.

## PHASE 2: ON-PREMISE CUSTOMER USE

A limited number of financial institutions have moved into this phase by making biometric technologies available for customer use. Concerns about customer adoption and privacy issues are key factors inhibiting adoption, but such concerns are slowly disappearing since September 11. As a result, financial institutions are likely to move into this phase much sooner than one may have expected even a year ago. Surprisingly, credit unions have been the quickest to offer biometric technologies to their customers in the United States, with the majority of other deployments of this type being launched overseas. To date, customers have primarily used the technology in branches to identify themselves to tellers, to authorize transactions, and at ATM and check-cashing kiosks.

The following are examples of financial institutions that have announced Phase 2 deployments:

- **Purdue Employees Federal Credit Union** was one of the first financial institutions to deploy biometric technologies for use by its members by installing finger-scanning technology in its self-service kiosks. The kiosks were created as a less expensive alternative to opening additional branches. They enable users to perform such transactions as opening new accounts and applying for loans.
- **Charles Schwab** is currently using signature verification for opening new accounts in more than 300 of its brick and mortar locations.
- **Bank United** has integrated iris recognition into a number of its ATMs.

### PHASE 3: REMOTE USE BY CUSTOMERS

The final phase of the technology evolution will be for customers to use the technology for tasks, such as home banking and day trading, performed from their homes and from remote locations. This will require customers to have access to their own personal biometric devices. This phase will take a long time if the financial burden is left to the customer. Therefore, it is likely that financial institutions will attempt to encourage usage by either providing the technology to their customers free of charge or at deep discounts. There are few examples, to date, of home deployments with the exception of biometric access to PCs and PDAs, and voice authentication in conjunction with telephone banking, the technology most favored for remote access.

The following are examples of financial institutions that have announced Phase 3 deployments:

- **BACOB Bank** in Belgium is piloting voice verification for customer account access.
- Signature verification technologies are currently available on some laptops and PDAs for login.

### OTHER AREAS

Biometric technologies are making great strides in several other areas of financial services.

**Point-of-sale payments.** Point-of-sale payments, especially in conjunction with credit cards, provide a large market for biometric developers, as it is necessary to find ways to prevent fraudulent use of stolen cards. Finger scanners and signature verification provide a good fit for this type of usage. Finger scanning devices are low in cost and can easily be set up at retail counters. Hypercom, a leading provider of credit-card processing devices, has already developed a biometric finger-scanning pad that attaches to its terminals and can be used to identify a cardholder's identity at point of sale. The device costs about \$120 per terminal to buy and install. Two merchants have already agreed to test it early this year. The company sees this as a good alternative to smart cards which have not been very successful in the United States.

Signature verification, on the other hand, seems like a natural fit for point-of-sale payments as the card user must sign their name anyway. Many credit card companies have already begun to take a serious look at the potential of this technology. E-payments solutions provider CardinalCommerce, for example, recently teamed with signature verification developer Communication Intelligence Corporation (CIC) in an effort to provide merchants and consumers with secure biometric verification for credit card transactions. Under the agreement, CIC's signature verification technology will be integrated in CardinalCommerce's

Payment authentication platform. The platform is also currently undergoing testing with MasterCard International's Secure Payment Application.

**Smart Cards.** Smart cards have been slow to take off, especially in the United States, but when they do, they will offer a good partnership for biometrics. The integration of Recognition Systems Inc. (RSI) hand-geometry technology with a smart card provides a good example of how these technologies can be used in combination. The smart card reader, which is attached to RSI's HandReader, stores the user ID and biometric hand template on the smart card. When a user presents the card and places their hand in the hand reader, it compares measurements such as hand length, width, thickness and surface area with the template stored in the smart card in order to verify identity. Since the smart card stores the user's hand template, it eliminates the need to distribute the hand templates across a network of HandReaders. For companies with multiple locations, this allows employees to access several facilities without having to be enrolled at each site.

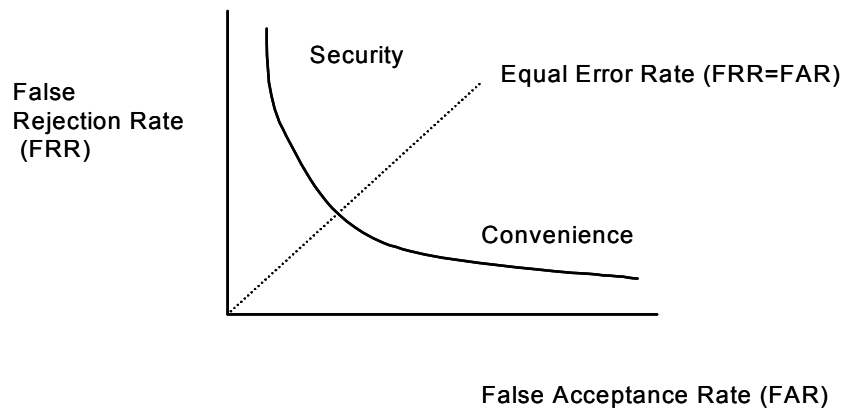
---

## CHOOSING THE RIGHT BIOMETRIC DEVICE

Advancements in technology over the last few years have enabled most devices to achieve very high levels of accuracy with only slight differences between them. However, no biometric device is 100% accurate, and accuracy levels reached in testing environments are not necessarily consistent with real life situations.

Accuracy levels are often measured in one of two ways in the biometrics industry: by a false rejection rate (FRR) or by a false acceptance rate (FAR). The FRR gives the percentage of instances an authorized individual is falsely rejected by the system. The FAR gives the percentage of instances a non-authorized individual is falsely accepted by the system. While an institution wants both percentages to be low, a decrease in one will always be at the expense of the other, as the two are diametrically opposed. Institutions have the ability to adjust FRR and FAR levels to better meet their needs. As Figure 4 illustrates, a higher FRR and a lower FAR, for example, leads to greater security, while the opposite provides greater convenience. So, while accuracy is of course very important, there are other factors that an

**Figure 4: FRR and FAR are Diametrically Opposed**



Source: Nuance

institution must consider when choosing the appropriate device to suit their needs.

- **Cost** is an important consideration to many organizations, especially since large-scale deployments can become quite costly. High implementation costs have actually been a deterrent for many organizations considering implementing biometric technology. Today, however, as a result of improvements in technology and more widespread usage, costs have come down significantly. For example, finger-scanning devices, which at one time cost as much as \$1,000 apiece, can now be

purchased for approximately \$100, with many of the same, if not improved features. Decreases in cost have put the technology well within the budgets of even smaller organizations. Despite these lower costs however, as the table below shows, there still exists some degree of variance between different devices. It should be noted, however,

**Table 2: Comparison of Average Costs by Device Type**

Biometric Device	Average Cost
Face Recognition	\$250
Finger Scanning	\$100
Hand Geometry	N/A
Iris Recognition	\$240
Retina Scanning	\$2,000-\$2,500
Signature Verification	\$100 with digital tablet
Voice Authentication	\$50k for 4 port system and 4 weeks of professional service

*Source: Celent Communications and Vendors*

that it is difficult to compare device costs, as costs vary depending on application as well as volume. Table 2 merely provides average costs for single standalone devices.

Biometric technology should not be compared at face value to current security system costs. One should also take into account the cost of providing new passwords and replacing lost identification cards, as well as the cost of the human labor necessary to check identification cards in some cases—all of which can be eliminated with biometrics.

- **Location of devices.** It is essential to determine the way in which the technology will be used and where it will be located. Some devices work better in different environments. For example, while face-recognition vendors claim that the technology adjusts to different lighting and can identify an individual at different angles, this technology is probably not a good choice for access to an area that where lighting is inconsistent or insufficient. Another example would be deploying voice authentication technology in an area that is always noisy.
- **Users.** The best device to suit the needs of an organization will depend, to a certain degree, upon who is being authenticated. Acceptable levels of intrusiveness, ease of use, and accuracy requirements will obviously differ among constituents. For instance, customers are less

tolerant of delays and breaks in security than employees, who are in a less flexible situation and can be persuaded that biometrics are necessary despite the occasional false rejection; the other extreme would be biometric devices for prisoners, where one would expect the highest levels of accuracy with a low tolerance for false identification. Further complicating the decision is the fact that some biometric devices do not work well with people of certain ethnic groups or fields of work. For example, physical laborers such as construction workers and gardeners tend to have poor-quality fingerprints, making finger-scanning and hand-scanning technologies a poor choice. Asian women also supposedly have less defined ridges in their hands, making those technologies a poor choice for them.

- **Size of organization.** Most biometric devices today have both verification and identification capabilities. It is therefore important to consider the size of the organization and the expected number of potential users of the device. Cost, processing speed, and fewer false acceptances make verification a more popular choice. It is also a better technique for a larger user base. If the comparison parameters for an identification search are loosely defined, the search may match more than one user to the same data. From a convenience standpoint however, identification is the preferred method because the user is not required to provide any additional identification other than the biometric sample.

---

## FUTURE TRENDS

**Increased Acceptance.** To date, most large financial institutions have at least begun to pilot biometric technologies. Deployments have not been on a large scale, but as institutions become more comfortable with the technology, they will not only use it to a greater degree, but will also make it more available for use by their customers (Phase 2 deployment). Industry players are optimistic about market potential and future adoption rates and are looking to the large financial institutions to lead the way. These institutions will serve as models for the industry. Their acceptance of the technology, as well as their success with it, will encourage other institutions to follow. Increased acceptance and adoption will quickly pull the industry out of its infancy, creating a more mature market where only best-of-breed developers are likely to survive.

Greater acceptance will also come as a result of education. While people are more willing to sacrifice privacy and intrusiveness for a greater sense of security, the public needs to be educated on the benefits of the technology in order to eliminate misperceptions and fears surrounding the technology. Developers as well as trade organizations such as the International Biometric Industry Association (ABIA) in Washington, D.C., are also helping to promote public awareness and serve as advocates for the industry. Financial institutions will play a major role as well, by encouraging their customers to use the technology when it is available, by running promotions, and by providing benefits to early adopters just as they have with other new services, such as online banking and electronic bill payment. Home usage of biometric devices for account access and ecommerce will be adopted more quickly if financial institutions and card companies are willing to provide free or discounted devices.

**Proven ROI.** September 11 has certainly opened up the biometrics market. In order to succeed, however, the technology must prove itself, not only from a security perspective but also through a high return on investment to justify the necessary capital outlay. Greater focus has been placed on ROI as companies continue to cut IT budgets during recessionary times. Lengthening corporate decision cycles also pose a challenge to technology vendors. When evaluating biometric technologies, it is essential that institutions not look simply at the cost of the technology but also recognize the money saved by elimination of passwords, call center requests, and staff needed to manually check identification cards.

**Industry Standard.** One factor that has prevented the biometrics industry from really taking off and maturing has been the lack, up until recently, of an industry-wide standard that would enable products from one vendor to work with the products of another. Such a standard prevents deploying institutions from having to spend large sums of money to build new systems from scratch each time they launch a new vendor biometric product, and also provides systems integrators with greater flexibility when selecting products. The standard

enables the flexible deployment of biometrics across platforms and operating systems. Vendors will also benefit from more markets to sell their products which in turn will lead eventually to lower costs.

The new standard is called BioAPI (Application Programming Interface) and was created by the BioAPI Consortium. The consortium was formed in April 1998 with the intention of developing an API for the industry, according to the notion that interoperability is necessary for an industry to mature. Version 1.1 of the standard was released in March 2001, and it is currently backed by more than 85 companies, including biometric developers, systems integrators, and OEMs. The existence of BioAPI is hugely significant for the industry and is yet another factor pushing the industry forward.

**Consolidation and Integration of biometric devices.** As with all growing industries, consolidation often comes into play as competition intensifies. Leaders are already beginning to emerge and some of the smaller players are likely to disappear. There has already been some evidence of consolidation within the industry with the most recent announcement coming last month from Identix and Visionics. This planned merger also illustrates another trend likely to develop within the industry: multiple offerings. Developers are not only faced with the challenge of proving their dominance within their individual sector but also of demonstrating the benefits of their device type over others. In doing so, many are realizing that although their products are strong on a stand-alone basis, even greater security can be achieved when multiple devices are used together. Different devices work well in different environments and BioAPI will enable integration within a single infrastructure. Going forward we are likely to see vendors as well as devices working together. In order to achieve the highest level of security, financial institutions are likely to evaluate factors such as need, user base, and environment and they are likely to consider implementing several types of biometric devices at once.

**Partnerships with integrators.** Despite decreasing device prices, costs continue to be a barrier to widespread deployment of biometric technologies. However, integration companies such as Protocom offer institutions the ability to deploy biometric technologies in a more cost-effective manner with a faster ROI. Integrators give an organization single sign-on capabilities. They partner with biometric developers to make that single sign-on a biometric one, rather than a more vulnerable password. The resulting cost-savings from the elimination of multiple log-ons as well as passwords altogether offset the cost of deploying the product. In addition, companies like Protocom use a generic template which does not lock the institution into a particular biometric device or vendor. In this way the institution can continue to add to its initial deployment and get the most from its investment. Partnering with integrators is likely to be a promising path for many developers as it will offer them a new channel through which to sell their products.

**Conclusion.** While great strides have been made within the biometrics industry over the last few months, some giant steps have yet to be taken. The vulnerability of passwords and

consumer demands for greater security are causing the industry to mature rapidly. Financial institutions are demonstrating increased interest through pilot programs and deployments. A new standard is likely to result in smoother implementations and decreased costs. As the market opens up and awareness is heightened, it is now up to the biometric developers to deliver on their promises.

---

## ABOUT CELENT

Celent Communications is a research and advisory firm dedicated to helping financial institutions formulate comprehensive business and technology strategies. Celent publishes reports identifying trends and best practices in financial services technology, and conducts consulting engagements for financial institutions looking to use technology to enhance existing business processes or launch new business strategies. With a team of internationally experienced analysts, Celent is uniquely positioned to offer strategic advice and market insights on a global basis.

Celent's research services cover the following eight sectors of financial services: Retail Banking, Wholesale Banking, Retail Trading, Institutional Trading, Personal Insurance, Commercial Insurance, Mobile Financial Services, and European Financial Services. For inquiries, visit [www.celent.com](http://www.celent.com); email [info@celent.com](mailto:info@celent.com); or contact:

**Headquarters:**

183 State Street, Fifth Floor  
Boston, MA 02109  
USA  
Tel.: +1.617.573.9450  
Fax: +1.617.573.9455

489 Fifth Avenue, 12th Floor  
New York, NY 10017  
USA  
Tel.: +1.212.490.2220  
Fax: +1.212.490.2225

50 California Street, Suite 1500  
San Francisco, CA 94111  
USA  
Tel: +1.415.439.5291  
Fax: +1.415.439.5299

16, Place Vendôme  
75001 Paris  
France  
Tel.: +33.1.53.45.28.58  
Fax: +33.1.53.45.28.29