BIOMETRICS RESEARCH GROUP, INC.

Mobile Biometric Authentication White Paper

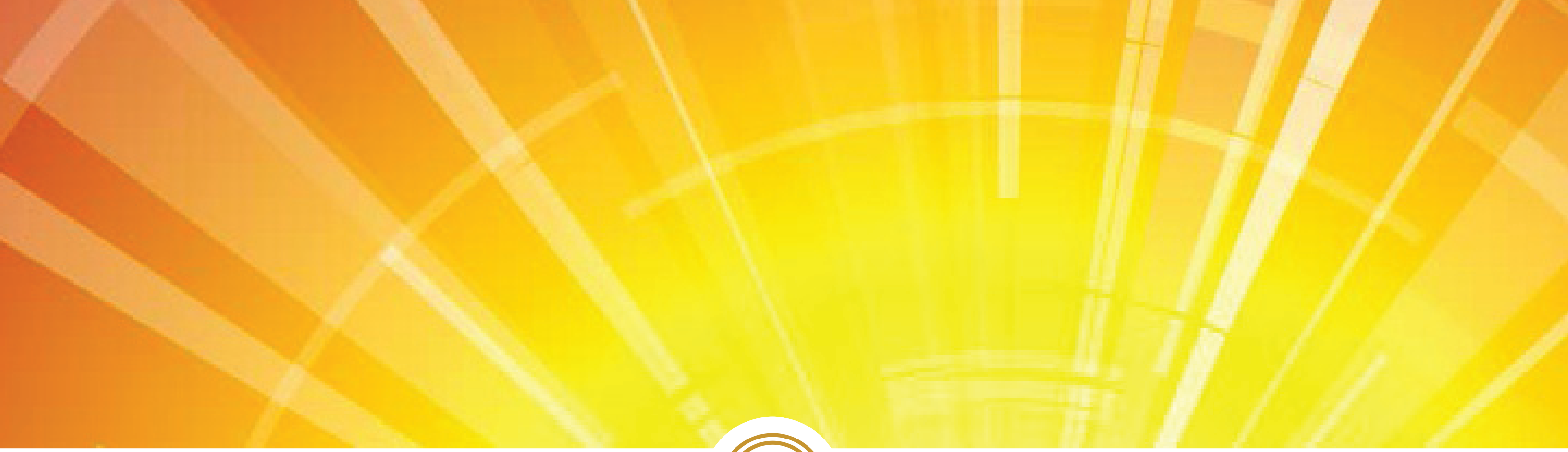
This report examines how the total market for mobile biometrics will increase due to smartphone growth along with the drive for password supplantation. This report also outlines the increasing use of mobile biometrics for financial services and to aid in law enforcement and military applications.

Rawlson O`Neil King
Lead Researcher, Biometrics Research Group, Inc.

All information, analysis, forecasts and data provided by Biometrics Research Group, Inc. is for the exclusive use of subscribing persons and organizations (including those using the service on a trial basis). All such content is copyrighted in the name of Biometric Research Group, Inc., and as such no part of this content may be reproduced, repackaged, copies or redistributed without the express consent of Biometrics Research Group, Inc.

All content, including forecasts, analysis and opinion, has been based on information and sources believed to be accurate and reliable at the time of publishing. Biometrics Research Group, Inc. makes no representation of/or warranty of any kind as to the accuracy or completeness of any information provided, and accepts no liability whatsoever for any loss or damage resulting from opinion, errors, inaccuracies or omissions affecting any part of the content.

© 2014, Biometrics Research Group, Inc.



AGNITiO

Voice iD

Secure . Universal . Natural

TABLE OF CONTENTS

Research Methodology

Biometrics Research Group, Inc. uses a combination of primary and secondary research methodologies to compile the necessary information for its research projections.

The conclusions drawn are based on our best judgment of exhibited trends, the expected direction the industry may follow, and consideration of a host of industry drivers, restraints, and challenges that represent the possibility for such trends to occur over a specific time frame. All supporting analyses and data are provided to the best of ability.

Primary Research

Biometrics Research Group, Inc. conducts interviews with technology providers, clients, and other organizations, as well as stakeholders in each of the technology segments, standards organizations, privacy commissions, and other influential agencies. To provide balance to these interviews, industry thought leaders who track the implementation of the biometric technologies are also interviewed to get their perspective on the issues of market acceptance and future direction of the industry.

Biometrics Research Group, Inc. also applies its own proprietary micro- and macroeconomic modeling using a regression analysis methodology to determine the size of biometric and related-industry marketplaces. Using databases of both publicly and privately-available financial data, Biometrics Research Group works to project market size and market potential, in the context of the global economic marketplace, using proven econometric models.

Secondary Research

Biometrics Research Group, Inc. also draws upon secondary research which includes published sources such as those from government bodies, think tanks, industry associations, internet sources, and Biometrics Research Group, Inc.'s own repository of news items. This information was used to enrich and externalize the primary data. Data sources are cited where applicable.

Defining Mobile Biometrics

Mobile biometrics refers to the deployment of biometric authentication methods on mobile devices such as smartphones and tablets.

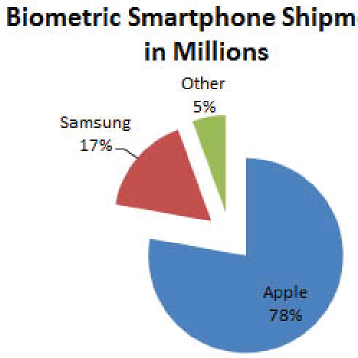
Use cases for mobile biometrics include securing sensitive data on personal or corporate mobile devices, such as enterprise or financial information, providing physical access to corporate facilities and providing mobile identity management tools to national security and law enforcement agencies.

Over the past few years, mobile devices such as smartphones and tablets have become a key computing platform, transforming how people access business and personal information. Due to the large number of new smartphones expected to ship in 2014, Biometrics Research Group expects that the smartphone mass market will drive rapid growth in consumer electronics biometrics.

Smartphone Growth

Biometrics Research Group, Inc. estimate that smartphone manufacturer shipments in the U.S. were 79 million in 2011, rising to 155 million units in 2014, growing to 175 million units in 2018.

Sales of smartphones in the U.S. were nearly 60 million in 2011, will be 120.5 million this year and will grow to be relatively flat at 121 million in 2018. Active subscribers (otherwise referred to as the "installed base") was 115 million in 2011, is estimated to be 240 million in 2014 and will grow to be 279 million in 2018. Some analysts estimate the number of U.S. subscribers will exceed 300 million in 2018, but these usually include a number of inactive units, units being retired and other units being recycled and distributed elsewhere (typically in other developing markets).



Copyright © 2013 Biometrics Research Group, Inc.

Due the proliferation of smartphones in the U.S. market, biometrics is quickly becoming an essential consideration for smart mobile devices. With the increasing functionality and services accessible via mobile telephones, there is a strong argument that the user authentication level on mobile devices should be extended beyond the personal identification number (PIN) that has traditionally been used.

One of the principal alternatives that the industry has focused upon is the use of biometric techniques on mobile phones as a method to verify the identity of a person accessing a service. We consider biometrics as measurable physical and behavioral characteristics that enable the establishment and verification of an individual's identity. Biometric patterns can be anything from fingerprints, iris scans, facial recognition, voice recognition and more.

Biometrics Research Group, Inc. predicts that there will be a rush by smart mobile device manufacturers to integrate biometrics technology into their next generation devices. Biometrics Research Group projects that over 90 million smartphones with biometric technology will be shipped in 2014. The Biometrics Institute also found in its 2014 Industry Survey a significant rise in the use of biometrics among mobile devices over the past year.

Goode Intelligence has forecast that by 2019 there will be 5.5 billion users of mobile and wearable biometric technology around the globe.

According to its Mobile and Wearable Biometric Authentication: Market Analysis and Forecasts 2014-2019 report, Goode Intelligence projects growth will initially be driven by the integration of fingerprint sensors in high-end smartphones and tablets. Growth will then be rapidly followed by other innovative biometric technologies deployed as part of either FIDO Aware solutions, proprietary-device OEM led initiatives such as Touch ID, and integration into multi-factor authentication platforms.

The forecasted spike in popularity will be brought on by the fact that wearable technology offers great potential to support biometric technology for authentication purposes.

Goode Intelligence goes on to further predict that Apple will integrate biometrics into its "iWatch smart watch" later this year, either in the form of its Touch ID fingerprint solution or another biometric modality such as heartbeat recognition.

The report also highlights key drivers behind the adoption of mobile and wearable biometric authentication, which include: convenient authentication; replacing password and PINs; driving mobile payments; and securing enterprise mobility, which is main authenticator for the Internet of things.

"We believe that smartphones and tablets will be the first wave of consumer devices to be biometrically-enabled and this will quickly be followed by wearable technology" Alan Goode, author of the report and founder of Goode Intelligence said.

"We are very much at the beginning of another transformational aspect of authentication – the use of wearable technology for authentication purposes, in particular leveraging the next wave of biometric technology to create seamless, continuous, authentication. What will be truly transformational about the use of biometrics on wearable devices, is the birth of the universal authenticator – a device that intuitively knows who we are, where we are, what we want to do and can open doors – both physical and virtual."

Goode Intelligence has also projected that 619 million people will be using biometrics on mobile devices by the end of 2015. Goode also predicts that by 2017, there will be more than 990 million mobile devices with fingerprint sensors.

Biometrics Research Group, Inc. also notes that Apple is currently the leading manufacturer of biometric-enabled mobile devices. This is because Apple was the first manufacturer to introduce biometric technology to the global smartphone mass market. In 2013, Apple released its newer upmarket iPhone 5S with a fingerprint identity sensor, entitled Touch ID, built directly into the device's home button. This new generation premium Apple smartphone features a capacitive sensor that is 170 microns thin, 500 ppi resolution that can scan sub-epidermal layers, and has a 360 degree readability capacity. The sensor is designed to unlock the iPhone and facilitate purchases.

Using an adaptive system, which Apple obtained through the purchase of AuthenTec Inc., the iPhone sensor becomes more proficient at reading fingerprints the more it is used. AuthenTec specialized in offering content and data protection, access control and strong fingerprint security on mobile devices. By acquiring the firm in 2013, Apple obtained most of foundational technology patents in the fingerprint biometrics segment, along with a broad patent portfolio consisting of 200 issued and filed patents in the United States.

Apple's acquired technology patents outline the implementation of an embedded sapphire crystal sensor, that can encrypt fingerprint data directly into the iPhone's new A7 64-bit processing chip, so that biometric information will not be stored in the cloud.

Biometrics Research Group, Inc. believes that the development of Apple's embedded touch fingerprint sensor was a pivotal moment for the biometrics industry, which has ultimately spurred the acceleration of mobile biometric products.

Our research firm projects that the inclusion of biometrics in mobile devices will generate about US$9 billion worth of revenue by 2018 for the biometrics industry, not just through unlocking mobile devices through security applications, but also through multi-factor authentication services and the approval of instant electronic payments.

In fact, Biometrics Research Group, Inc. believes that the widespread use of biometrics in consumer electronics will ultimately act as a catalyst for total industry revenue growth. Currently, the Biometrics Research Group predicts that biometric smartphones will increase the compound annual growth rate for consumer electronic biometrics by at least 35 percent over next five years. A major contributing factor in this growth will be increasing demand for personal devices that can conduct safe financial transactions.

In March 2013, the Biometrics Research Group estimated that U.S. consumers would use smartphones and tablet computers to make retail purchases of approximately US$35 billion that year, compared with US$20 billion in 2012. If that trend continues, we projected that the majority of online sales would be conducted on Apple rather than on Android mobile devices. As a consequence, we expect that Apple could ultimately integrate fingerprint authentication into “Apple ID” services to supplement the written password that provides access to all Apple cloud-based services, including iTunes purchases.

Mobile Biometrics Adoption and Password Supplantation

Biometrics Research Group and other noted market research and technology firms eventually expect that biometric identifiers such as fingerprints will eventually supplant written Apple ID passwords. We believe that this will occur because biometrics are conceivably provide a more secure method of authentication for online computing resources and financial services. As online services become more prevalent, more organizations will use biometrics as a security measure.

Gartner predicts that by 2016, 30 percent of organizations will use biometric authentication on mobile devices, up from five percent today.

“Mobile users staunchly resist authentication methods that were tolerable on PCs and are still needed to bolster secure access on mobile devices,” said Ant Allan, research vice president at Gartner. “Security leaders must manage users’ expectations and take into account the user experience without compromising security.”

Gartner also recommends that security leaders evaluate biometric authentication methods where higher-assurance authentication is required. Suitable authentication modes include interface interactivity, voice recognition, face topography and iris structure. These modes can be used in conjunction with passwords to provide higher-assurance authentication without requiring any significant change in user behavior, the group says.

Moreover, as a mobile device itself provides a rich node of identity-relevant contextual data, this information can also be used to increase the trust in the claimed identity. It is possible that the combination of passive biometric authentication and contextual authentication will provide sufficient assurance in medium-risk scenarios without the need for “gateway” authentication events using passwords or tokens.

IBM also believes in the trend of replacing passwords with biometric authentication. David Nahamoo, IBM’s chief technology officer, stated in speech in late 2011 that he expected that biometrics would replace passwords by 2015.

“Over the next five years, your unique biological identity and biometric data – facial definitions, iris scans, voice files, even your DNA – will become the key to safeguarding your personal identity and information and replace the current user ID and password system," stated Nahamoo. "We have been moving from devices like desktops and laptops to smart devices such as mobile phones and tablets – all property that is easily lost, stolen or misplaced. These devices are not yet outfitted with operating systems and security elements that are as strong as immobile devices of the past. Biometric security can strengthen those weaknesses."

In 2006, Microsoft had released a fingerprint scanner device to allow users to access its operating system without a password, while in 2012 Google released a facial recognition feature to allow users to access their Android-based smartphones. While both of these technologies are rudimentary and have been subjected to security breaches, they both are harbingers of how we will access a constellation of smart telecommunication and computing devices in the future, along with other applications, such as personal banking.

IBM also predicts that biometrics will eventually integrate with a wider number of commonplace technologies available in today's consumer electronics to enhance security.

"We can take advantage of the advanced technology being used in the smart devices, such as microphones, touch screens and high definition cameras to fully employ biometric security options," states Nahamoo. "While there is already some adoption of facial and voice recognition, combining these and other biometric data points in the near future can eliminate the hassle of memorizing, storing and securing account IDs and passwords and at the same time give users a greater security confidence."

As a result of this industry approach, it could be technically feasible to purchase new Apple devices at its retail stores using a thumbprint impression in the near future. Biometrics Research Group also expects that biometric technologies will also be integrated to "phablets", or niche mobile smartphone/tablet hybrids, which are extremely popular in Asia.

In short, we predict that biometrics will become integrated within a wide number of mobile devices within this upcoming smartphone product release cycle. Biometrics Research Group had also predicted that this integration will be driven by smartphone and tablet manufacturers such as Apple and Samsung Electronics.

As previously discussed, Apple integrated its fingerprint identity sensor into its iPhone 5S product. Biometrics Research Group then correctly anticipated that Samsung would follow by introducing biometric recognition in its new set of mobile devices as well. In February 2014, Samsung launched its Galaxy S5 smartphone with an expected embedded fingerprint sensor. The smartphone runs Android 4.4.2 (Kitkat), and features a 2.5GHz Quad core processor along with 5.1" FHD Super AMOLED display. The fingerprint sensor is of the swipe variety, and has been embedded beneath the home button on the GS5.

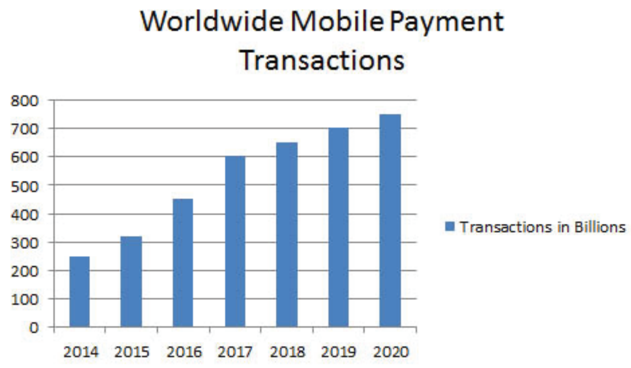
In May 2014, Samsung followed up by announcing its intentions to incorporate biometric sensors into the majority of its mobile devices, including low-cost smartphones. Samsung noted that a market leader, it intends to follow the market trend by examining various types of biometrics for user authentication, including iris detection.

As a result, we expect that both iris and fingerprint recognition will also ultimately be integrated into both Apple and Samsung's respective smartphones and tablets.

Mobile Biometrics Adoption and Financial Services

Biometrics Research Group, Inc. expects that mobile commerce adoption will accelerate due to impending wide-scale integration of biometric technology into smartphones.

The research consultancy predicts that worldwide mobile payment transactions will reach US$250 billion in 2014, reaching US$750 billion in annual transactions with more than 700 million users by 2020. We see biometrics as a transformative force that will speed mobile commerce, especially in North America, because the technology can offer a higher level of security, while providing an intuitive customer experience.



Copyright © 2013 Biometrics Research Group, Inc.

Biometrics Research Group also estimates that at least three-quarters of current smartphone users do not secure their devices with a passcode. The use of instinctive technology such as fingerprint recognition will allow consumers to easily secure their devices and make payments. The integrity of a payment process without a physical payment card is quickly compromised if a device is not secured. One goal of mobile biometrics will therefore be to secure the user login process in order to enable more dependable user identification.

Challenges however remain with obtaining this goal for business applications. Access to business data from mobile de¬vices requires some form of secure authentication, but traditional password schemes based on a mix of alphanumeric symbols are cumbersome and unpopular, leading commercial firms to prohibit their employees from accessing business data on their personal mobile devices altogether.

Samsung is beginning to attempting to address this issue with the introduction of Knox. Samsung Knox provides security features that enable business and personal content to coexist on the same handset. In its current version, user press an icon that switches from "personal" to "work" profiles immediately, with no delay or reboot wait time. Samsung has claimed this feature will be fully compatible with Android and Google and will provide a full separation of work and personal data on mobile devices and address all major security gaps in Android.

Our research finds that the healthcare and the financial sectors are taking advantage of Knox. However, Samsung wants wider penetration of paid Knox subscribers. While the mobile security platform is embedded on 87 million devices, only 1.8 million users have actively deployed the system for regular use. The implementation of iris recognition in Samsung mobile products might increase Knox usage.

Firms are continuing to examine new ways to leverage mobile technologies in order to leverage integrated technologies for biometric authentication. The rich set of input sensors on mobile devices, including cameras, microphones, touchscreens, and GPS, enable sophisticated multimedia interactions. Biometric authentication methods using these sensors can provide a natural alternative to password schemes, since the sensors are fa¬miliar and already are used for a variety of mobile tasks. By combining biometric capabilities such as a fingerprint readers or voice recognition software with mobile devices that users carry with them all the time, enterprises in the future will be able to deploy two-factor authentication as part of an enterprise-class identity and access management infrastructure.

Potential corporate uses include granting access to security-enhanced silos of enterprise data or applications stored on the device, requiring on-device biometric scans to authenticate the user to the enterprise network and applications, and possibly even granting physical access to buildings. Such mobile biometric application models can also be used to authenticate client interactions with banks and other financial institutions.

Biometrics Research Group believes the driving "push" factor for adoption is that biometric technology shortens transaction time. It provides security unlike other measures used. Using biometrics can prevent Internet fraud, money laundering, and identity theft. Consequently, many financial institutions in emerging economies, over the past year, have been electing to use biometric technologies, such as automated teller machines (ATMs), in their retail banking operations.

Global Industry Analysts (GIA) believes that the total market for biometrics for banking will exceed US$8 billion by 2020. According to GIA, the market leading up to 2020 will be driven by an increased emphasis on protecting financial transactions from fraud and security breaches.

Though still in its emerging stages, biometrics is increasingly finding application in financial services and banking institutions in various Asian countries. The technology is being used to enhance customer service and for identity verification and for preventing identity theft in financial transactions. GIA also finds that government efforts in emerging nations to promote the use of banking by people with less access to financial services will additionally drive gains in the market.

While biometric technologies are mostly accepted at ATMs in Asia, they are not in North America due to legal and customary differences. Surveys however have found that biometrics in banking in North America would be more quickly embraced in order to secure financial services on mobile devices.

Andrews Research recently conducted a survey on behalf of the Deloitte Center for Financial Services on mobile devices and the financial services industry. The survey found that 72 percent of respondents would welcome the use of biometric identification, such as fingerprints or eye scans, to enable a mobile device, such as a tablet or smartphone, for financial transactions.

For banking security, over half of survey respondents endorsed "preclearance" of a limited number of people who could receive a limited dollar amount of funds vis-a-vis mobile payment. Two-thirds of respondents also supported leveraging a mobile device's GPS for real-time, location-based fraud sensing and prevention.

Analysts at Deloitte who authored a report based on the survey findings concluded: "Implementing such concrete security measures, then calling attention to such efforts in advertising and social media campaigns designed specifically to address such concerns, could perhaps help overcome lingering consumer hesitations about accessing personal financial information or transacting financial business over smartphones and tablets."

Despite consumer concern over mobile device security in the financial sector, the survey found that 63 percent of smartphone users had interacted with their bank through a mobile app.

While more respondents have used apps for banking, less than half of that percentage have used apps for insurance and investment management. Among insurance customers, approximately three-quarters of survey respondents stated they did not use mobile devices to display an insurance card or file a claim. Indeed, the survey found that 65 percent of respondents with a life insurance policy were not sure whether their carrier offered a mobile app. Sixty-three percent of those with homeowner's or renter's insurance, as well as 57 percent of auto insurance consumers were also not aware of mobile app options.

For investment management and brokerage customers, more than half did not check their balances or positions on mobile devices, while 80 percent revealed that they did not trade securities through mobile apps. Nearly half of survey respondents were also not sure whether their mutual fund, retirement account, or investment account providers offered mobile apps.

In terms of value, 39 percent of those surveyed characterized the ability to deal with their bank on a mobile device as extremely or very important, versus only 23 percent for investment-related activities and just 19 percent for insurance.

Based on these findings, Deloitte analysts concluded that: "Financial services companies should look for ways to use the increasing ubiquity of mobile technologies to cultivate deeper customer engagement and boost brand loyalty." A method to increase this ubiquity will most likely include enhanced security and user authentication driven by biometric technologies.

The biometrics industry is responding to the "ubiquity" challenge by developing mobile biometrics software platforms and standards that ensure enhanced authentication, especially for access to financial services.

In April 2014, Diamond Fortress Technologies launched a new touchless biometric fingerprint authentication software development kit (SDK) for enterprise mobile applications – for both iOS and Android development. According to the company, the new SDK – called ONYX HD3 provides a high level of security by using a mobile device's rear-facing camera to take a picture of a finger and proprietary algorithms to identify prints. The SDK also now features auto-capture.

Also in April, AGNITiO updated its own KIVOX Mobile platform, which is a SDK which enables on-device secure speaker verification. It can be easily integrated in authentication applications for smartphones and other embedded platforms. Enrolment and matching are done locally. There is no need for network connections or voice transmissions. As a result, authentication can be done anywhere.

Users can select a predefined passphrase or choose its own, in any language, to create a Biometric Voice Print (BVP) which can later be used for verification. KIVOX Mobile offers a successful detection rate of more than 99.5 percent, with a false acceptance rate of less than 0.1 percent. On top of this, with the use of AGNITiO's proprietary patented anti-spoofing technology, KIVOX Mobile detects up to 97 percent of replay attacks, as well as many other spoofing attacks such as cut-and-paste. The protection is achieved as part of the verification attempt, without the need for any additional steps such as liveness detection.

Late in 2013, BIO-key International launched a new system for fingerprint authentication, which the company says allows integrations to accommodate and expand on concepts embodied in mobile biometric platforms. Called FreeChoiceID, the BIO-key says it has created an entirely new approach to mobile authentication privacy. FreeChoiceID leverages BIO-key's patents on in storing biometric and related key data, and BIO-key's patented secure transport of biometric and secondary form-factor user authentication data between devices and across public or private networks. Expanding upon BIO-key's patented WEB-key platform, FreeChoiceID ensures consumer and enterprise user authentication data is secured as it is moved between a device and cloud-based services, and that data is properly protected when it is used by WEB-key.

The primarily intent of this model is to give users control over the privacy of their biometric data – controlling where it is stored, in what form as well as which applications have access to it. Using the BIO-key FreeChoiceID mobile application, users of a BIO-key integrated application can approve or deny each access to their biometric data by any BIO-key application even when it is stored on a server in a public or private cloud, the company says.

Other biometric firms are also working on more limited mobile apps, rather than full-fledged platforms that take advantage of biometric sensors in mobile devices.

Sensory has just launched TrulySecure, a new mobile app that supports on-device biometric authentication using speaker verification and facial recognition. According to the company, Sensory's new approach uses the existing microphone and camera in smartphones, so it is accessible for users of lower-end devices. Considering authentication happens on the device, Sensory says there is no need for a cloud connection, which could slow things down. The company also notes that this makes biometric data more secure. "Consumers generally find it cumbersome to use PINs and passwords to lock their phones, and as a result these devices often go unlocked," said Todd Mozer, CEO of Sensory. "Sensory's biometric authentication provides a high level of security, while still being convenient and fast enough that people will use it."

Mobile Biometrics and "The Internet of Things"

Using biometric authentication on mobile devices will therefore enhance both consumer security and the consumer experience. The enhancement of security will be increasingly important as cloud-based services available on mobile devices become ubiquitous.

Ubiquitous computing is a paradigm in which networked computing resources are extended beyond traditional conceptions of computing. Users augment their computing and communication capabilities with a range of computing devices, which potentially allows the network to become an infinitely accessible environment for those specific users. Resources are mobile and have both hardwired and wireless connectivity.

In such a scenario, computer services and devices make use of information processing that can be easily obtained through nearly any microprocessor-based device. The benefit of structured extensibility is based on the fact that computers, consumer electronics, sensors and computerized networks are increasingly pervasive. The growing use of computers as a part of a larger collection of devices leads to a change in perception in which computers are not just singular machines on a single network. Instead, computers are implanted into a wide array of everyday devices and all of these devices are bound together by a broad range of communication technologies, providing the infrastructure for these devices to be tools of greater economic integration.

This array is increased referred to as the "Internet of Things". The "Internet of Things" can be defined as a diffuse layer of devices, sensors, and computing power that overlays the entire Internet.

Traditionally, the Internet has been defined only by computing and networking equipment, but now the "Internet of Things" paradigm proposes the inclusion of a wider array of devices, once overlooked.

This new paradigm will potentially connect any electro-mechanical device to the Internet with identifying devices or machine-readable instruments. For instance, business may no longer run out of stock or generate waste products, as they could know exactly which products consumers need. A person's ability to interact with objects could be altered remotely based on immediate or present needs, with this in mind.

Biometrics Research Group, Inc. estimates that the "Internet of Things" will account for an increasingly large number of connections, from nearly two billion devices today, climbing to nine billion connections by 2018.

The "Internet of Things" is possible through a framework of "structured extensibility."

Structured extensibility extends networks by integrating a broad range of technologies into a network of economic relationships. The network logic is based on information grids that are in turn, based upon distributed and ubiquitous computing facilities that connect industries and markets, increasing the rate of potential economic growth.

The process of structured extensibility allows all these devices to interact, creating new technological arrangements, in which information is created and exchanged. This new framework leverages web services, which are technologies designed to give consumers a greater level of interactivity through this network of devices.

Applications that cannot be accessed except by following rigid, traditional computing approaches are made accessible using the same infrastructure that enabled the widespread use of web technologies. The result of this is that enhanced Internet services are no longer restrained to computing devices. A new generation of Internet services, based upon web services, extends commercial and financial services to a wide host of consumer electronic devices and even biometric sensors.

Biometric Research Group, Inc. estimates that a growing proportion of "Internet of Things" devices will be constituted by biometric sensors. We conservatively estimate that biometric sensors will total at least 500 million "Internet of Things" connections by 2018. Many of these devices will be mobile in nature.

Mobile Biometrics and Military and Law Enforcement Applications

Mobile biometrics also refers to the proliferating front-line mobile technologies that aid military, law enforcement and border security agencies in identifying people in the field. Based around a central biometric identification system, mobile biometric identification devices extend the functionality and capabilities of a static identification system by allowing users to capture fingerprints and facial images, or to compare fingerprint minutiae templates or images against a biometric database, either stored locally on the device, or remotely in centralized biometric matching systems.

Captured information can also be compared with that stored within radio-frequency identification (RFID) tags, smart cards and other machine-readable identification documents. In scenarios where information is stored remotely, the mobile biometric identification device communicates with a central database using common wireless technologies such as 3G, Wi-Fi or Bluetooth. If a positive match, known as a 'hit', is made during the comparison process, information associated with the individual in question, such as facial images, names and demographic data, is transmitted back to the mobile device.

Mobile biometric identification devices are designed for intuitive operation, and incorporate a reader, scanner and camera for the capture of a biometric identifier, such as fingerprint or facial images, which is then converted by software into digital format for storage and comparison against other records held in a biometric identification system database. With top-tier mobile biometric solutions, images are analyzed for quality prior to capture and encoding, ensuring the best possible inputs for biometric matching.

One of the leading providers of mobile military and border security biometric reader technology is Cross Match Technologies.

In August 2011, the firm teamed with GTSI, a provider of technology solutions to federal, state, and local governments, to supply Biometric Automated Toolset under contract for the U.S. Army. This contract was for mobile biometric devices that would assist soldiers in real-time identification of persons of interest on the battlefield. The contract had a total value of US$159 million. The award covered a 16-month period and was executed as part of GTSI's Information Technology Enterprise Solutions 2 Hardware (ITES-2H) contract with the federal government.

The Biometric Automated Toolset includes an enrollment kit consisting of a laptop and attached biometric collection devices capable of enrollment, verification, and identity detection, together with mobile handheld devices for collecting, storing, and uploading pertinent data to U.S. Army biometrics collection centers. A system of servers containing the biometric database maintains and synchronizes information, ensuring that data collected at one location is available at others. News reports in 2011 demonstrated that the 17th Infantry Brigade, which is part of the First Army Division, completed a seven-day biometrics training course using the enrollment kits.

The U.S. Army launched a weeklong training program to help integrate biometric technologies into the mobilization program of the U.S. Army. The U.S. military has gone on record to state that biometrics is an important tool that can separate friend from foe on the battlefield. Biometrics will be a key technology for deployed personnel engaged in future urban terrain operations.

The brigade engaged in a 40-hour training program focused primarily on how to operate the biometric equipment. Soldiers were taught how to correctly enroll and identify individuals, along with the proper management of their data files. A team comprised both military and civilian experts who taught the course.

The fielding of military grade biometrics equipment is currently occurring in Afghanistan. Forward operation personnel will see their old handheld Interagency Detection Equipment replaced with the Secure Electronic Enrollment Kits. The kit, which is called SEEK II, has been extensively tested.

The kit not only enrolls an individual but also launches a simultaneous search to determine if a person is on a watch list. The new hardware also has improved fingerprint recognition and iris image capture capabilities. Soldiers at the ground level are expected to collect not only usable biometric data but also enroll civilians who are willing to submit themselves.

U.S. Marines have been using the mobile biometric capture device from Cross Match in battlefield scenarios. Entitled the Biometric Enrollment and Screening Device (BESD), it has already enrolled over 19,000 persons of interest in Afghanistan.

Specifically, the Marines are using the SEEK II which was reportedly used to identify Osama Bin Laden. Of the 19,000 persons of interest identified with the SEEK II, the Marines say 300 have been placed on a watch list. According to military sources, more than 2,000 Marines and coalition soldiers have received training with the device between 2012 and 2013. The SEEK II records fingerprints, iris scans and a facial image. At least 15,000 units have reportedly been shipped to U.S. military personnel around the world.

Also last year, Cross Match launched its new SEEK Avenger mobile handheld unit, aimed at immigration, customs, border control, law enforcement and security communities. The new device incorporates Cross Match's MOBS software, as well as secure credential reader and communication options. Forty percent smaller than the SEEK II, the SEEK Avenger weighs just over three pounds and according to the company, is the only multi-biometric handheld capable of capturing stand-off dual iris (SAP 40) and fingerprint (FAP 45) images in direct sunlight..

A built-in contact card reader and optional MRZ and ePassort readers provide users the flexibility to configure their optimal credentialing solution. A 5MP camera provides 1D/2D barcode reading, captures evidentiary photos and video, and takes facial images utilizing auto-facial recognition. The optional communications cap incorporates into the device, providing LTE/3G or other network certified cellular modems for additional connectivity beyond Bluetooth and Wi-Fi.

This new addition to the SEEK family runs Cross Match's MOBS Software on a Windows-based OS and incorporates onboard matching against a watchlist of up to 250,000 records. The onboard software also generates multiple agency-compliant files and handles the transmission of these files for remote matching to regional or national AFIS databases, as required.

Conclusion

With the technology world transitioning from PC-based to mobile computing, Biometrics Research Group, Inc. expects security will become a key consideration for protecting personal, corporate and financial data. Consequently, we expect mobile biometrics to increasingly be embraced by both mobile device manufacturers and by consumers as mobile technology and mobile commerce continues to evolve and become pervasive.

Previously, Biometrics Research Group, Inc. accurately predicted that biometrics would become integrated within a wide number of mobile devices during the last smartphone product release cycle. Now, another prediction is proving accurate.

In a Biometrics Research Note issued in March 2013, the research vendor stated it believed that by next year, biometric fingerprint identifiers would eventually supplant written Apple ID passwords: "By 2015, it might become possible to purchase new Apple devices at its retail store using a thumbprint impression." In July 2014, BiometricUpdate.com reported that Apple is preparing to launch an "iWallet" app allowing customers to easily make retail payments through their mobile phones. The new app will reportedly leverage the firm's Touch ID fingerprint sensor to verify a customer's identity.

Apple has already told some of its partners that the new iPhone will include a "secure element" system that will allow it to store sensitive data such as financial credentials. This secure element system is expected to be the same secure system that currently stores the user's fingerprint data and has the ability to store future mobile health data. Apple is apparently also looking to operate the system without giving up control to wireless carriers.

Recent news item also claim that dialogue between Apple and credit card vendors, including Visa, concerning the new mobile commerce application has heated up in recent months. Sources briefed on the talks say that Apple executives are discussing the launch of a mobile wallet application as soon as the autumn to permit consumers to use their iPhones to purchase goods in brick-and-mortar retail stores.

The launch of the mobile wallet application would be timed to coincide with the launch of the long-rumoured iPhone 6 in October. This time horizon would allow Apple to build popularity and market share for the iWallet app on the lead-in to the holiday shopping season and the New Year.

Mobile payment transaction growth, combined with biometrics, will ensure increased speed of mobile commerce, especially in North America, because the technology can offer a higher level of security, while providing an intuitive customer experience.

About the Biometrics Research Group, Inc.

Biometrics Research Group, Inc. provides proprietary research, consumer and business data, custom consulting, and industry intelligence to help companies make informed business decisions.

We provide news, research and analysis to companies ranging from Fortune 500 to small start-ups through market reports, primary studies, consumer research, custom research, consultation, workshops, executive conferences and our free daily BiometricUpdate.com news service.

Biometrics Research Group has positioned itself as the world's preferred supplier of pure-play market research and consultancy services focused on the biometric marketplace, which particular focus on the law enforcement and national security sectors. Our portfolio of white papers and full research reports is based upon high-quality quantitative analysis, allowing our clients to gain deeper understanding of the marketplace.

We customize our research design, data collection, and statistical reporting using proprietary micro- and macroeconomic modeling and regression analysis.
Through integration of our research results with qualitative analysis from our BiometricUpdate.com news service, we provide actionable business analysis.