Mobile Biometric Applications

BIOMETRIC UPDATE.COM

Rawlson O'Neil King Lead Researcher, Biometrics Research Group.
Chris Burt, Contributing Editor, BiometricUpdate.com

About the Biometrics Research Group

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 in 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.

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.

FIDO® Face Authenticator

- High-performance facial recognition
- Active and passive spoof detection
- Several integration options
- Android and iOS support
- FIDO® Certified Client and Server also available

fido CERTIFIED UAF

AWARE

+1.781.276.4000 | sales@aware.com

www.aware.com/fido

Executive Overview

Mobile biometric applications operate on mobile devices such as smartphones and tablets, with "apps" utilizing embedded software and sensors to make secure use of those devices and apps more convenient. They do so by enabling the owner of a device to use their biometrics to authenticate their identity as an enhancement or alternative to passwords.

Mobile biometrics will continue to experience exponential growth due to increased consumer demand for convenient security, particularly where secure use of mobile devices is especially critical, such as for mobile banking and commerce. Adoption of standards such as FIDO® will further drive competition, innovation, and ultimately adoption of new biometric authentication methods.

Market Synopsis

In 2018, Biometrics Research Group, Inc. projects that revenue associated with mobile biometrics will total US$10 billion based on 3.2 billion users. This projection has increased from our last research report on mobile biometrics, in which we projected that biometrics in mobile devices will generate approximately US$9 billion worth of revenue by 2018 for the biometrics industry.

Biometrics Research Group continues to believe that mobile biometrics will transition between 2015 to 2020 from a consumer adoption phase to full maturity, enabling the technology to overtake existing authentication technologies. By 2020, we estimate that biometrics will be ubiquitous, installed in 100 percent of mobile devices. This transition would meet IBM's 2010 prediction that biometrics would ultimately provide all security authentication capabilities for individuals using mobile devices within five years.

A driving force for the wide implementation of mobile biometrics will be the continued: rapid expansion of smartphone users. Biometrics Research Group, Inc. estimates that smartphone manufacturer shipments in the U.S. were 79 million in 2011, rising to 155 million units in 2014, and will grow to 175 million units by 2018. Sales of smartphones in the U.S. were nearly 60 million in 2011, will be 120.5 million in 2014 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).

Acuity Market Intelligence published its 'Biometric Smartphone Update' in January 2017, which estimates that the number of smartphones incorporating fingerprint or eye-based biometrics globally has doubled since January 2016. Their report finds that "87 smartphone vendors have introduced 346 biometric smartphones in the past year," which brings the total number of biometric smartphone models introduced since 2013 to 549.

This figure is more than double the 200 models that Acuity Market Intelligence reported in January 2016. In addition, the report finds that the quarterly average price of a biometric smartphone dropped from $849 to $277 from 2013 to 2016. There are also 127 biometric smartphone models selling for $150 or less.

"The proliferation of biometric smartphones is extraordinary. The 500 models currently available on the market today represent a ten-fold increase in just two years," said Maxine Most, Acuity Market Intelligence principal. "Biometric smartphone growth will continue as mobile application security, particularly for financial services, demands biometric authentication, low-cost apps and sensors drive down the cost of biometric integration, and consumers clamor to eliminate their reliance on passwords and pins."

The report also states that nearly one billion biometric smartphones are currently in use, which comprises 40 percent of the overall global smartphone market.

This market share is expected to escalate to 100% of the two billion smartphones shipped annually within two years reaching 100% installed base penetration by 2022, Acuity said.

Biometric smartphones entered the market in 2014, initially with 28 vendors offering mostly one model. Today, of the 87 vendors offering biometric smartphones, more than 30 offer at least six models while ZTE, Huawei, Lenovo, Samsung and Xiaomi have each introduced at least 20 models.

"This unprecedented growth supports Acuity's assertion that within two years, biometrics will be as ubiquitous on smartphones as high resolution cameras are today," Most said. "Acuity is confident the market will achieve the 100% biometric smartphone penetration originally forecast for the end of 2018 in The Global Biometrics and Mobility Report. This will not only fundamentally change the dynamics of the smartphone market but create a truly global platform for biometric authentication."

The "Biometric Smartphone Update" report shares information about all biometric smartphones models including biometric mode, vendor, and sensor, as well as brand, OS, price, introduction date, availability, and links to specifications and reviews.

Acuity Market Intelligence has also published new research that predicts that by 2022, annual production of biometric "physical" identity credentials will peak at more than one billion a year.

Worldwide, Biometrics Research Group estimates that the number of total smartphone users worldwide will surpass 3 billion in 2017. Continuing growth of the global smartphone user base along with the consumerization of biometrics will drive the growth of mobile biometric authentication. We project that inexpensive smartphones will open new opportunities for marketing and commerce in emerging markets, where many consumers previously had no access to the Internet. Meanwhile, in mature, established markets, smartphones will rapidly shift the paradigm to more consumer media usage and toward more enterprise-centric mobile usage.

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

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

Analysts generally predict that there will be a rush by smart mobile device manufacturers to integrate biometrics technology into their next generation devices. According to its Mobile and Wearable Biometric Authentication: Market Analysis and Forecasts 2014-2019 report, Goode Intelligence projected growth would be initially 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, which will be discussed later in this paper, and by proprietary-device OEM led initiatives such as Touch ID, and integration into multi-factor authentication platforms.

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 familiar and already are used for a variety of mobile tasks. By combining biometric capabilities such as a fingerprint reader 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.

Biometrics Research Group believes the driving "push" factor for mobile 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, over the past five years, have been electing to use biometric technologies in their retail banking operations. Over that period, we have observed

the adoption of banking applications on mobile phone platforms that leverage TouchID and other biometric technologies to authenticate bank account holders.

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. The technology will be increasingly used to enhance customer service and for identity verification, along with 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, as has been currently observed in India with its Aadhaar identification scheme.

With such a tremendous amount of growth projected in the industry, a key number of companies, as outlined below, have positioned themselves as product and service leaders in the mobile biometric space.

Aware, Inc.

Aware is a veteran of the biometrics industry, providing a comprehensive portfolio of biometrics software products since 1993 for fingerprint, face, and iris recognition applications ranging from defense and border management to mobile authentication. We specialize in providing for top-tier biometric analysis, processing, and matching algorithms, provided in products that are easy to use with world-class technical support. Our FIDO® Client, FIDO Server, and FIDO Face Authenticator products are FIDO® Certified. Our mobile face authenticator performs robust spoof detection and high-performance matching for easy, reliable, secure authentication.

EyeVerify

EyeVerify, Inc. is a biometric security technology company based in Kansas City, Missouri. Its chief product, Eyeprint ID, provides verification using eye veins and other micro-features in and around the eye. Images of the human eye are used to authenticate mobile device users.

Eyeprint ID is a highly accurate biometric technology for smart devices that delivers a password-free mobile experience with convenient, secure, private authentication. The patented solution uses the existing cameras on mobile devices to image and pattern match the blood vessels in the whites of the eye and other micro features in and around the eye.

EyeVerify licenses its software for use in mobile

banking applications, such as those offered by Tangerine Bank, NCR/Digital Insight and Wells Fargo.

The company is a wholly-owned subsidiary of Ant Financial Services Group, also known as Zhejiang Ant Small and Micro Financial Services Group Co., Ltd., a Chinese company. With the vision "to turn trust into wealth", Ant Financial Services Group is dedicated to building a leading data and technology platform to make financial services accessible to consumers and small businesses globally.

EyeVerify is a member of the FIDO Alliance and the International Biometrics & Identification Association.

Veridium

Veridium is a leading provider of end-to-end biometric authentication designed to safeguard enterprises' most critical assets.

Veridium's solutions ensure a secure environment for complete protection of biometric data and communication between mobile devices and back-end servers. Built on an open standard, it is one of the most flexible solutions on the market today.

Powered by a long legacy of biometrics R&D, Veridium solutions help organizations to increase security, reduce fraud, and cut the costs associated with passwords and traditional multi-factor authentication solutions. Veridium has offices in the U.S., U.K., Netherlands, and Romania.

The company was formerly known as Hoyos Labs but relaunched as Veridium, along with launching it VeridiumID solution, to offer enterprises a way to completely replace passwords with face, voice, and fingerprint authentication.

As Hoyos Labs, the company received eight patents, and it has another 34 pending. Now, as Veridium, it will apply some of that research and development to a product offering focused on enterprises in the Global 2000, financial services, healthcare, and government.

Veridium also differentiates itself by offering an open standard to encourage development with its products.

Apple

Consumer electronics giant Apple is 9th on the global Fortune 500. The company manufactures and sells computers and mobile devices, along with software and cloud services to support them. It earned over $230 billion in revenue in 2015, and employs over 100,000 people globally. Mobile devices, including phones, tablets, and wearables, have long been the main source of revenue for Apple, and as such it has been a major contributor to increasing consumer awareness and adoption of biometrics.

Apple's signature iPhone series began including a fingerprint sensor with the 5S in 2013, and the sensor has evolved with subsequent models. The company's mobile devices on its proprietary operating system also represent one of the top platforms for mobile biometric applications, taking advantage of embedded features such as the camera, for facial or iris recognition, and the microphone, for voice recognition. It also added its Touch ID fingerprint authentication to MacBook Pro laptops in 2016.

Apple received several patents and filed others relating to biometrics in 2016, and is continuing to innovate integrated hardware and software solutions for consumers. Current examples of Apple's biometric research and development include research released by the company on training artificial intelligence for accurate facial recognition by creating realistic fake images in December, and its development of a heart-based biometric sensor.

BioEnable

BioEnable manufactures hardware and develops software for fingerprint scanners. In addition to fingerprint scanners, the company provides dual iris scanners and access control products.

The company is based in Pune, India, and was founded in 2001. It serves government and corporate customers in over 50 countries, and has over 100 employees.

BioEnable released its fingerprint scanner SDK and Android drivers in 2012 to allow mobile phones to be used as a replacement for dedicated handheld terminals. The SDK enables connections to single or multiple-finger scanners. The company has also designed mobile dashboards and applications for identification, automation, and tracking on both Android and iOS platforms.

It is a major supplier of devices for use with the Aadhaar Project, India's national unique identification program, which has enrolled over a billion people. BioEnable is a leading provider of fingerprint recognition and security systems in the Asia Pacific region, and has over 20,000 installations, according to the company.

In addition to biometrics, BioEnable has also launched products based on Active RFID and GPS tracking technologies. In Europe, BioEnable offers research and development services for identification and wireless technologies.

Fingerprint Cards

Fingerprint Cards globally provides fingerprint chips for smartphones and tablets, as well as algorithms, processors, and modules. President and CEO Christian Frederikson estimated the company's market share for fingerprint sensors in mobile units at between 55 and 60 percent in 2016.

Fingerprint Cards sensors are found in numerous mobile devices, including Google, Motorola, Lenovo, Huawei, Xaiomi, and Meito smartphones, and Samsung notebooks. It provides touch sensors for glass, ceramic, and spray displays, and for front, back, or side placement for mobile devices.

Fingerprint Cards went public in 2002 and is traded on the Nasdaq Stockholm exchange. It reported year-end revenues of SEK 6,638 million (approximately US$740 million) for fiscal 2016, and is forecasting a 2017 revenue of SEK 7,500-9,500.

The company recently acquired iris recognition firm Delta ID for $106 million to expand its capabilities beyond fingerprint recognition. In 2016 Fingerprint Cards formed a partnership with Zwipe to develop the market for biometric smartcards for the payment industry.

The company was founded in 1997, and is based in Gothenburg, Sweden. It has over 300 employees, and branch offices in Sweden, Denmark, South Korea, China, Japan, Taiwan, India, and the U.S. It also has distributors in more than a dozen other countries.

Google

Google is a subsidiary of Alphabet, and supplies many of the world's most popular mobile applications, in addition to its search, advertising, and enterprise cloud, and hardware businesses.

The Android mobile operating system for smartphones, tablets, and wearables has the largest number of installations of any operating system, and while open-source, it was developed by Google. Android is supported by biometric products provided by many companies, including Suprema and Precise Biometrics, and it is a supported platform for many applications, including ones from Digital Insights, Nok Nok Labs, NexID Hyundai, and Net-X Solutions.

Google Pixel smartphones include the Trusted Voice feature, which allows users to unlock their Android devices with voice recognition, as well as fingerprint sensors manufactured by Fingerprint Cards. Mobile users can also authenticate to make purchases from the Google Play Store by fingerprint with some devices. Google's mobile payment platform, Android Pay, also supports fingerprint authorization.

Among biometric projects currently in development, it provides a speech recognition API from its Google Cloud Platform, which is currently in beta testing, and the company has also run a pilot project for face biometric authentication for payments. Face recognition is part of Google's Smart Lock system, which Google is planning to extend with behavioural biometrics in 2017 under its Project Abacus, which it says is much more secure than fingerprint authentication. It is also developing fingerprint support for its Chrome laptop OS.

Alphabet is traded on the NASDAQ and has a market capacity of approximately US$582.4 billion.

Google was founded in 1998, employs 57,000 people, and is based in Mountain View, California.

Nuance

Nuance provides desktop and mobile software for individuals, businesses, health care providers, and developers.

Their products provide the Dragon line of speech recognition applications, including Dragon Anywhere mobile dictation for Android and iOS. It also offers Nuance Identifier, Nuance Monitor, and Nuance Forensics voice identification applications.

Mobile voice recognition products include the VoCon Hybrid SDK for embedded and connected voice recognition, and the VoCon Speech Signal Enhancement (SSE) suite of signal processing technologies.

The Nuance Security Suite enterprise fraud prevention solution features behavioural biometrics from BioCatch for continuous authentication via its FraudMiner interface. Addition of this feature followed the company's acquisition of voice biometrics firm Agnitio by Nuance to become part of the security group of Nuance's enterprise division.

Nuance is expecting major growth in India over the next two years, fuelled by demand for voice biometric authentication in mobile banking services. Nuance voice authentication technology is currently used by a number of financial companies, including HSBC in the UK, Eastern Bank in Massachusetts, and the Virginia Credit Union.

The company is also developing products for IoT and connected living.

Nuance is publicly traded on the NASDAQ, and has a market capacity of $4.97 billion.

Originally founded in 1992 as Visioneer, and also formerly known as Scansoft, Nuance is based in Burlington, Massachusetts, and has 12,000 employees in 35 offices worldwide.

Precise Biometrics

Precise Biometrics provides fingeprint technology and Tactivo smart card readers.

Its fingerprint solutions include Precise BioMatch Mobile for smartphones and tablets, Precise BioMatch Embedded, featuring small sensors and limited platforms for smart cards, wearables, and IoT devices, and national ID and smart card fingerprint algorithm Precise Match on Card.

Precise Biometrics products are used by smartphone vendors, the U.S. federal government, international enterprises, and large healthcare providers.

Integrations of Precise Biometrics fingerprint solutions into several smartphones, including the Meitu M6s, were announced in 2016 and early 2017. Companies that signed licensing agreements with Precise Biometrics in 2016 include Samsung System LSI Business, Image Match Design Inc., InvenSense Inc. and Vkansee.

Fingerprint Cards was Precise Biometrics' biggest client, selling its fingerprint sensors with Precise Biometrics algorithms for use in smartphones, but sales to Fingerprint Cards are slated to end in 2017.

Precise Biometrics reached an agreement to acquire NexID Biometrics in early 2017 for US$3.49 million to add its spoof mitigation and liveness detection technology to its capabilities, and will integrate liveness detection with Precise BioMatch Mobile in the first half of the year.

The company was founded in 1997, and is based in Lund, Sweden. It went public on the Stockholm Stock Exchange in 2002, and reported consolidated net sales of SEK 97.2 million (US$10.9 million) in 2016, up 72 percent from SEK 56.3 million (US$6.3 million) from 2015.

Safran Identity & Security

Safran Identity & Security is a global leader in identity and security solutions, deploying systems in more than 100 countries.

Backed by more than 40 years of experience in biometrics, the company develops innovative technologies for the public and private sectors, including identity management, secure transactions and public security solutions.

The global firm's biometric solutions help individuals, governments and businesses protect identities and ensure privacy, in an increasingly digital world. The firm provides civil identity management, systems for public security and authentication of online transactions.

The company has a number of operating divisions, including MorphoTrak, a U.S. leader in secure multi-biometric technologies for fingerprint, face, and iris recognition, which provides comprehensive biometric solutions to government agencies along with statewide AFIS solutions. MorphoTrak is also the vendor of choice to supply matching algorithms for the FBI's NGI system. And the firm is the only company in the U.S. that offers integrated border solutions using automated biographic and multi-modal biometrics technologies developed by Safran Identity & Security.

ValidSoft

ValidSoft is a voice and multi-factor authentication software provider, offering tokenless real-time authentication that is invisible to the customer and frictionless. ValidSoft is a subsidiary of Elephant Talk Communications Corp (ETAK), which announced in August 2015 that it would consider strategic alternatives including strategic disposition, joint venture, or merger transactions for the company.

It provides mobile voice verification solutions for call centers, e-commerce, online banking, healthcare and enterprise customers. ValidSoft software protects online, mobile, card, and telephone transactions for customers in financial services, government, and business automation.

ValidSoft offers APIs for all common mobile operating systems, as well as call centers, and web apps. Other solutions ValidSoft offers an operations, administration, and management layer, and hosting.

The company's device trust technology includes a real-time SIM Swap fraud detection service.

It announced a partnership to integrate as an authentication layer in AurionPro enterprise solutions in 2016, and signed several commercial customer contracts in 2015, including with ImageWare Systems and an unnamed U.S.-based corporation with over 100,000 employees.

ValidSoft is a member of the FIDO Alliance, and has an industry-leading four European Privacy Seals, as well as ISO 27001 certification for Europe.

The company was formed in 2003, is based in London, England, and has more than a dozen employees.

VoiceVault

VoiceVault provides voice biometric technology for use in mobile, on-device, and telephony applications.

Its flagship product is the ViGo mobile identity verification solution, which is a turnkey platform for mobile apps hosted on the Amazon Web Services cloud. Pre-built libraries are available for iOS and Android to accelerate mobile app development. It is available with a low cost entry point, and tiered pricing based on the number of users.

Other VoiceVault products include ViGo Wear for wearables, enterprise platform Fusion, which also supports ViGo, VoiceVault Identity Manager (ViM) for password reset and account unlocking, and VoiceSign, which provides e-signatures for mobile device transactions. It also provides solutions for call centers, out of band authentication, proof of life, and time and attendance tracking.

In benchmark testing, VoiceVault detected 99.98 percent of replay attacks among ten million calls. The company claims a success rate in production deployments of 99.9 percent, and has enrolled over a million voices from users in over 40 countries.

VoiceVault technology is used in solutions from BioConnect, SayPay, and Enacomm. It is also used by e-learning company Aceable.

VoiceVault was founded in 1996, and is a FIDO Alliance member. It is based in El Segundo, California, and has a research and development center in the UK.

Defining the Mobile Biometrics Market

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 have become a key computing platform, transforming how people access business and personal information. Access to business data from mobile devices 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 mobile devices altogether.

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 familiar and already are used for a variety of mobile tasks. By combining biometric capabilities such as a fingerprint reader 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 including 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.

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.

Mobile biometric identification devices are also typically defined by authentication methods. Given that biometric-enabled smartphones will reach 2.3 billion users by the end of this year, Biometrics Research Group believes authentication standards will change the definition of security and mobile payments experience overall. The following Aware white paper details some these emerging standards, along with technologies and strategies emerging concerning identity protection.

Biometric Authentication

Biometric authentication uses physical characteristics (fingerprints, voices, faces, etc.) as either an add-on or replacement to traditional passwords. Many current authentication methods do not provide the security that is actually needed. Passwords can be hacked and socially engineered from personal information that is readily shared on social media. PINs are not unique; the 20 most common combinations represent over 25 percent of in-use four-digit passwords.

As a consequence, reducing the value of passwords and instead utilizing unique physical characteristics, or biometrics, for identification is more beneficial.

Biometric single sign-on (SSO) is one such a biometric password management technology that secures passwords and networks and protects data from unauthorized access and security breaches.

Companies like Microsoft and Intel are implementing biometric authentication systems into their future products to protect user credentials, and organizations are now seriously considering multi-factor biometrics like fingerprint, retina, voice, retina, facial and heartbeat for authentication.

Banks have started working with leading technology firms in order to create authentication systems which are the key to a great mobile banking and mobile payments experience. By identifying a customer's face, voice and mobile device, biometric authentication makes it extremely difficult to spoof the true user.

The main aim behind this new authentication experience is to provide customers with secure and convenient banking. It will effectively remove the need of text-based passcodes from users.

There are different modes of biometric authentication including fingerprint, face, voice, iris, heartbeat, and others. Fingerprint biometrics is becoming mainstream with annual sensor shipments estimated at 1.4 billion units by 2020, up from 317 million in 2014, according to "Biometrics Go Mobile: A Market Overview" from Frost & Sullivan.

Biometrics Research Group contends that the market for automated fingerprint identification systems and fingerprint biometric technologies account for the greatest share of the global biometrics market and is forecast to continue to be the main source of overall market revenues from 2015 to 2020. The sector was valued at US$10 billion in 2015 and is expected to reach nearly US$25 billion in 2020.

Since biometrics cannot be stolen or crafted in the way that passwords can be, the result of innovation in the sector generally is that personal information has less value to would-be thieves. Tying accounts to our biometrics means that intruders can do little or nothing with the data they steal.

It is therefore arguable that biometrics will be the successor to the password as a tool for secure authentication. There are good reasons for that; biometrics are naturally unique and could hardly be more convenient. They enable strong authentication to become a seamless, transparent process that make login easier and more secure. But there are different ways to implement biometric authentication and they are not all created equal. Each has pros and cons for a given environment and application.

The most obvious alternatives in implementing biometrics are among the different "modalities" like fingerprint, face, eye, iris, voice, and keystroke; since they each have their own personality. For authentication on a mobile device, there are hardware-based constraints that dictate modality options, and not all devices on the market are the same, particularly across different geographical regions. Many smart phones incorporate fingerprint sensors and software used for authentication, and some are even introducing iris, which definitely has strong potential but requires infrared illumination of the eyes. But these are proprietary to the device; you get what you get, and they don't necessarily perform as desired for every application and environment (e.g., online shopping at a friend's house versus approval of financial transactions on a crowded subway car).

Biometric authentication can be implemented independently from those offered by the device, which is desirable for optimizing authentication performance and features for a particular application. Another benefit is that they can operate within and application more uniformly across different devices in terms of user experience and functionality. Biometrics implemented independently from the device use universal input peripherals such as the camera, microphone, and touchscreen instead of the authentication hardware and software offered by the device supplier. This can give an app provider more control over the desired functionality and performance. An approach emerging is to enable multiple modalities and give users a choice between which (one or more) to use.

Facial recognition can be used on any device with a front-facing camera, including smart phones, tablets, and laptops. Facial biometrics are convenient and popular with users, but can be more susceptible than other modalities to spoofing attacks, where a fraudster uses a digital image or video of their victim's face to impersonate them. It is important to implement robust liveness detection to reduce this risk.

Another alternative to consider is between a device- and server-centric approach; where to store enrolled reference biometric data and where to perform subsequent comparisons upon authentication attempts; on the device or centrally on a server. Each offers advantages and disadvantages in terms of security, performance, and functionality depending on the application, but both are likely to see widespread adoption.

In a device-centric model, a biometric comparison is performed on a mobile device or PC, which can then be used to satisfy a cryptographic challenge/response between the consumer and the relying party (the party relying on the authentication, such as a retailer). A leading standard for a device-centric model of authentication called "FIDO®" from the FIDO Alliance has been broadly advocated, and will likely emerge as a dominant mechanism for strong authentication on smartphones and PCs. Because device-based biometric authentication does not require central storage of biometric data, it can't lead to a large-scale breach where many biometrics are compromised at once. The FIDO approach offers additional security advantages over centrally stored passwords. But a lost or stolen device can always provide opportunities to attempt to defeat security measures and commit fraud.

A centralized, server-centric model requires storage of biometric enrollment data on a centralized server platform, and transfer of biometric data to the server for comparison upon an authentication attempt. This architecture might be used where stricter control of the authentication process, strength, and performance is desired, such as for managing employee access to a company's digital assets.

For both device- and server-centric models,

there is risk that in the event that biometric data is compromised, they no longer offer a secure authentication method, given their inherent permanence. But while it is possible that a physical biometric source (e.g., synthetic finger) be reproduced from a compromised biometric template and then used to spoof an authentication, it tends to be a tedious, unreliable, and detectable process, and it is becoming more so as anti-spoof technology matures.

"Renewable biometrics" have the potential to address that issue even more resoundingly. Here, biometric templates are encoded in a way that allows them to be matched in an obfuscated domain where the original biometric features are scrambled. Renewable biometrics are maturing and gaining adoption.

Biometrics enable secure authentication to be implemented with layers of challenge and risk to fraudsters that outweigh the value of the targeted asset. Like all security mechanisms, biometrics can be defeated with sufficient effort, but the barriers are high and are getting higher with techniques that make spoofing unattractive to the vast majority of even the most talented and ambitious fraudsters. Biometrics are particularly effective when combined with other approaches (e.g., the ability to erase a smart phone remotely), because they are so different; they have the effect of increasing not only the effort required to defeat security measures but also the variety of skills and knowledge required to do so. This is the essence of the power of biometrics as a complementary authentication approach.

Spoof Detection for Mobile Facial Biometrics

Because biometrics are emerging as a major complementary authentication technique, spoof detection is becoming a critical feature. While facial biometrics are convenient for mobile authentication, they also constitute a potential weakness, since the ubiquity of "selfies" makes them easy to attempt to "spoof" as biometrics. With the wide availability of smartphone cameras, facial images can be much more easily acquired and used to surreptitiously impersonate someone for the purpose of fraudulently accessing their devices and accounts.

While modalities like fingerprint and iris scan pose fairly substantial technical hurdles to spoofing, it is far easier for a fraudster to acquire the facial image of someone in the form of a digital photograph or video. Without sufficient precautions in place, images of someone's face can be used to impersonate someone simply by presenting an image or video of the victim's face in front of the camera during authentication, perhaps even using another mobile device.

This is why it is critical to implement strong liveness detection measures for facial authentication that recognize when a facial image is not a live, authentic selfie but actually a photo or video taken of the potential fraud victim. Approaches to spoof detection can be characterized as either "active", requiring interaction with the subject, and "passive" requiring no interaction.

For example, an active approach might include display of commands to the subject to move their head, blink, or change their expression. These commands might be random and unpredictable; this hurdle makes it much more difficult to use a canned photo or video to spoof. A passive approach does not require interaction with the subject. Rather, analysis is performed on the image or video that can detect image features that make it suspicious. Ideally, both approaches are employed simultaneously.

When accurate liveness detection features are in place and spoof detection is properly implemented, facial biometrics are a convenient and useful means to authenticate that effectively complement or even replace passwords. Aware, Inc., as an example, incorporates advanced facial spoof detection in its PreFace Mobile SDK for facial authentication, which is in turn included in several Aware authentication solutions such as its FIDO® Face Authenticator in FIDO® Suite.

FIDO has opened the door to more secure and convenient options such as biometrics to authenticate online. It is a good example of how standards can fuel innovation, particularly with strong leadership from industry and cooperation between both technology suppliers and consumers. By dividing the problem into

logical (i.e., market driven) parts and defining how those parts will work together, standards broaden access to a market exponentially, and adoption happens where healthy competition is enabled.

FIDO's UAF (Universal Authentication Framework) standards define three categories of functionality and how each interacts with the other: Client, Authenticator, and Server. That approach enables just about anyone with a secure and interoperable authentication mechanism to throw their hat into the ring. Note that FIDO didn't overprescribe with a modality requirement (e.g. face, fingerprint, eye, voice, keystroke, etc.), which likely would have had the opposite effect of commoditizing and stagnating the technology.

Identity protection and regulatory compliance

Identity authentication based on biometric matching continues to grow along with consumer acceptance in both private and public sectors. Biometrics, the unique physical characteristics that all human beings have, include fingerprints and iris scans, as well as facial and voice matching. These modalities can all be used – to various extents – to clearly identify and/or authenticate the identity of an individual. Where passwords and PIN numbers were once our primary security option, our own physical uniqueness has begun to transform the way we interact with our online world.

Once the domain of law enforcement only, biometrics will continue to grow in acceptance in commercial markets. Key to this acceptance and growth is the onboarding process – or the initial biometric capture process. An example is the growing number of traditional financial institutions who now request that new customers add one or more biometric characteristic during registration. This biometric could be a fingerprint, a voice sample, or an image of the customers' face. These unique characteristics become part and parcel, then, of the customer's interaction with the financial institution. Instead of entering a password, the user repeats a phrase (voice) or takes a selfie (face). Passwords can be lost and stolen. Faces cannot.

As well as offering convenience and security for consumers, biometrics also assist institutions with compliance to government regulations including Know Your Customer (KYC). KYC is the process of certain types of businesses verifying the identity of their client base – both new and existing. (The term also refers to the federal regulations that govern these activities.)

Identity documents can be faked. Identities and Social Security Numbers are widely available for purchase on the dark Web. This information can be used to repeatedly craft phony identities for fraudsters and terrorists to create new access. The addition of a biometric, however, changes the game. Once that unique physical characteristic is attached to an identity, it becomes extremely difficult for the new identities to be forged.

That said, the benefits for financial institutions and other commercial organizations are well understood. What about the consumer, though? Why would we agree to add an image of our unique physical characteristics to our personal accounts? There are actually several reasons why we would:

First, there is the convenience factor. Typing in long, multi-character passwords on a small smartphone keypad is much more difficult than entering a short PIN and taking a selfie. Also, as human beings we quite often forget our passwords. Our face is just always there.

Moreover, having a biometric tied to our personal accounts makes it much, much harder for fraudsters to take over our accounts. Our passwords can be stolen or guessed, and account takeovers are commonplace. Our biometrics are difficult to fake, but liveness detection measures are warranted. This makes our accounts more secure.

As a consequence, the benefits of biometric authentication can be clearly understood for both business and consumers. These benefits begin, as stated, with the onboarding process. In coming months and years, using your voice or face to transact online will become mainstream, particularly with younger "selfie" generations who are much more willing to trade the capture of a biometric for enhanced safety and convenience in transactions.

Mobile Authentication Will Deter Fraud

Some form of identity theft is at the heart of most financially-motivated fraud. A proliferation of personally identifiable information (PII) available through social media and other public sources is easily accessible to aspiring fraudsters, while the anonymity of Internet commerce and communication gives them plenty of cover.

Illicit call centers troll for private identity data from unsuspecting consumers and untrained customer service agents. Identity fraud is increasingly committed by sophisticated criminal organizations operating beyond the reach of outdated laws that do not address such crimes. "Mega-breaches" resulting in theft of vast quantities of identity information occur with regularity; many we surely never hear about. Synthetic identity fraud, based on skillful creation of fictional identities, is a significant and fast-growing source of losses to fraud. In short, identity fraud and its derivative crimes cost banks, retailers, healthcare providers, governments, and ultimately consumers and taxpayers around the globe hundreds of billions of dollars every year, and this figure continues to grow.

Biometrics are rapidly making their way into the mainstream as a means to help prevent such identity theft and fraud. Most visibly, fingerprint sensors are being integrated into smartphones as a more convenient mode of secure access to a device for its owner. These devices are increasingly enabling use of biometrics towards more secure mobile payment models that aim to avoid security pitfalls of credit cards.

Biometric authentication functionality provided in the recent Microsoft Windows 10 release can be used to secure access to external systems and websites, supporting fingerprint, face, and iris modalities.

Use of biometrics is growing because our fingerprints, faces, irises, and voices have truly special properties that make them an effective barrier to fraudsters attempting to surreptitiously impersonate us. They are useful because unlike names, ID numbers, email addresses, and passwords, they are comparatively more unique, secret, permanent, consistent, difficult to reproduce, and—most notably—physically bound to us, which also happens to be very convenient.

Biometric authentication on smartphones and other devices is effective and particularly useful to their owners to prevent their fraudulent use; biometrics are the password of the future. But from the perspective of a bank, government agency, or any organization aiming to broadly reduce its exposure to identity fraud, a more universal approach is needed to have a broad impact.

Here's why:

- Much of identity fraud is committed using 'synthetic' identities that are not stolen but created. Authentication alone does not address this type of fraud.
- Biometric verification does not verify the authenticity of identity data; only that the person verifying is the same who registered the data. Biometric verification on a device helps prevent a fraudster from using a stolen device to falsely claim the identity of the owner, but does not prevent them from establishing accounts with fraudulent information.
- Penetration of smartphones is growing rapidly, but is still on the order of only 36% globally according to GSMA Intelligence. In places where many people still don't use smartphones, other mechanisms are necessary to prevent identity fraud more universally.
- Authentication on smartphones is device-specific and constrained to operate as implemented by device, OS, and application suppliers. While organizations aim to standardize architecture and interfaces, biometric functionality and performance will not be universal or configurable on these devices, and will not necessarily meet the securty requirements of a particular application.

Fundamentally, there are many modes of identity fraud that simply can't be addressed by password enhancement, and types of accounts, applications, and environments that require more robust security and more trustable identity verification.

More than just “something we are”, biometrics allow us to permanently bind ourselves physically to digital information; a powerful capability that enables us to not only biometrically authenticate, but also to biometrically deduplicate; that is, to determine through biometric search whether someone is surreptitiously attempting to establish a false identity. Said another way, identity proofing with biometric search helps assure the integrity of our identity data: that one identity represents each person, that each person has only one identity, and that the identity data associated with a biometric can be trusted.

Robust identity proofing requires the enrollee to present identity documents and information in-person as part of an application or onboarding process. The process might additionally draw upon public and private data sources. A biometric enrollment and search performed as part of this process serves as a highly confident “duplicate check” to ensure that the applicant is not already registered in the system, perhaps with different identity information. If upon enrollment, a biometric search yields a match to an identity with different information than what is being claimed, there is reason for further investigation. This is the idea behind biometric identity proofing; a means to combat identity theft at its source by ensuring the integrity of identity data at the point of enrollment.

Once a duplicate check is performed, a biometric enrollment digitally links the enrollee’s trusted unique record to them physically through their biometrics. These biometrics can then be used perpetually to prevent future attempts at false representation of their identity information by a fraudster. The process also establishes a high level of trust in the authenticity of the identity data associated with the enrolled biometrics, making them more useful for future biometric authentications. While biometric identity proofing requires additional effort to verify identity data integrity and detect duplicate enrollments, it provides yet another very effective barrier to fraud.

Biometric identity proofing will emerge as a key identity fraud prevention approach; a means to validate the integrity of identity information at the time of collection. It will complement biometric authentication, enabling a higher degree of trust in the validity and uniqueness of the identity being claimed. It will be especially useful in deterring criminal schemes to defraud funds from chartered financial institutions and to protect commercial transactions.

Conclusion

The move by more smartphone manufacturers to embed biometric capabilities into their devices alongside interoperable authentication standards such as FIDO will contribute to the rapid and widespread adoption of mobile biometrics authentication technologies. Mobile biometric modalities will propagate due to increased smartphone sales and will mainly be used to protect mobile commerce and banking transactions.