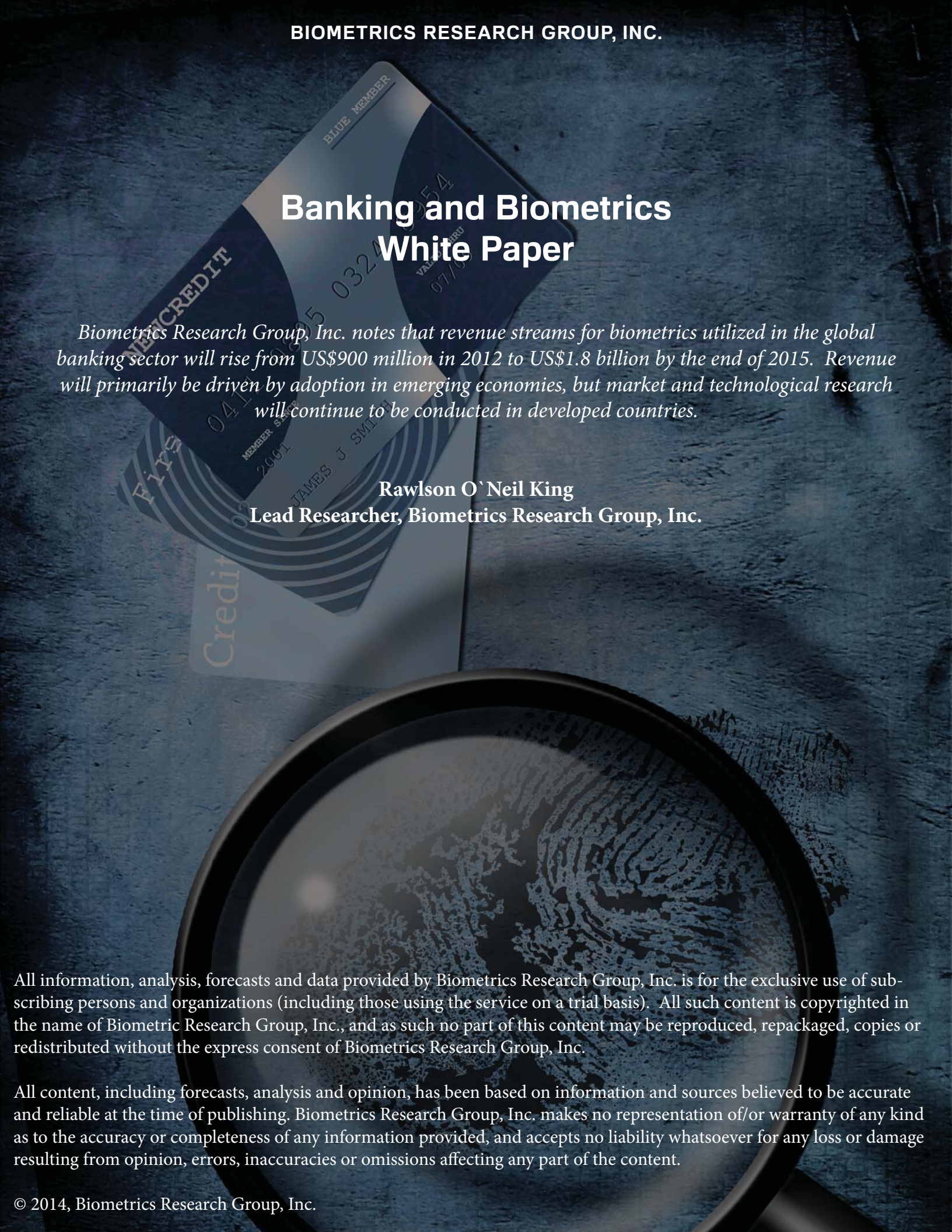

Banking and Biometrics White Paper

Biometrics Research Group, Inc. notes that revenue streams for biometrics utilized in the global banking sector will rise from US$900 million in 2012 to US$1.8 billion by the end of 2015. Revenue will primarily be driven by adoption in emerging economies, but market and technological research will continue to be conducted in developed countries.

Rawlson O`Neil King
Lead Researcher, 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.

Financial Institutions and Biometric Authentication

Many banks and other financial institutions around the world have implemented biometrics for client authentication. Biometrics is the science of recognizing an individual based on his or her physical and behavioural traits. Biometric-based authentication systems are widely considered to be more reliable than established password systems for verifying individuals and ensuring they are who they say they are.

Biometrics Research Group, Inc. defines 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, palm prints, gait, facial recognition or even voice recognition. **We estimated that total revenues for biometrics supplied to the global banking sector totalled US$900 million by the end of 2012.**

Countries such as Brazil, India, Poland and Japan already support automated teller machine (ATM) cash withdrawals by means of biometrics, while many other countries intend to follow the trend in the near future, especially in Asia and Africa. While security experts, especially in North America, are cautious about the use of biometrics in the highly regulated banking industry, financial institutions continue to implement biometric solutions as a countermeasure to address problems of identity theft and fraud.

Biometrics Research Group projects that revenue growth surrounding biometrics in the global banking sector will be driven by an increased emphasis on protecting financial transactions from fraud, identity theft and security breaches. **We estimate that total revenues, based on this demand will ultimately increase to US$1.8 billion by the end of 2015.**

Growing Risk of Identity Theft & Banking Fraud
A major exemplar that will drive increased security requirements is the problem of identity theft and other banking fraud. According to the U.S. Department of Justice, approximately seven percent of persons age 16 or older were victims of identity theft in 2012.

The U.S. government states that the majority of identity theft incidents (85 percent) in the United States involved the fraudulent use of existing account information, such as credit card or bank account information. About 14 percent of identity theft victims experienced out-of-pocket losses of $1 or more. Of these victims, about half suffered losses of less than US$100.

Of those who reported a direct financial loss, victims who experienced the misuse of their personal information reported a mean direct loss of US$9,650 and a median direct loss of US$1,900. Victims of new account fraud incurred an average loss per incident of US$7,135 and a median loss of US$600. Victims of multiple types of fraud reported an average direct loss of $2,140 with a median direct loss of US$400, while victims of existing account misuse had an average loss of US$1,003 per incident with a median direct loss of US$200. In addition to any direct financial loss, six percent of all identity theft victims reported indirect losses associated with the most recent incident of identity theft. Victims who suffered an indirect loss of at least US$1 reported an average indirect loss of US$4,168, with a median of US$30. With the exception of victims of personal information fraud, identity theft victims who reported indirect financial loss had a median indirect loss of US$100 or less.

Identity theft victims reported a total of US$24.7 billion in direct and indirect losses attributed to all incidents of identity theft experienced in 2012. These losses exceeded the US$14 billion victims lost from all other property crimes (burglary, motor vehicle theft, and theft) measured by the National Crime Victimization Survey in 2012. Identity theft losses were over four times greater than losses due to stolen money and property in burglaries (US$5.2 billion) and theft (US$5.7 billion), and eight times the total losses associated with motor vehicle theft (US$3.1 billion). According to the U.S. Federal Trade Commission, there is a new victim of ID theft every three seconds.

Due to these types of security challenges that are endemic in all countries, banks and other financial institutions around the world are increasingly considering the feasibility of biometric authentication for

TABLE 1

Persons age 16 or older who experienced at least one identity theft incident in the past 12 months, by type of theft, 2012

	Anytime during the past 12 months[a]		Most recent incident[b]		
Type of identity theft	Number of victims	Percent of all persons	Number of victims	Percent of all persons	Percent of all victims
Total	16,580,500	6.7%	16,580,500	6.7%	100%
Existing account	15,323,500	6.2%	14,022,100	5.7%	84.6%
Credit card	7,698,500	3.1	6,676,300	2.7	40.3
Bank	7,470,700	3.0	6,191,500	2.5	37.3
Other	1,696,400	0.7	1,154,300	0.5	7.0
New account	1,125,100	0.5%	683,400	0.3%	4.1%
Personal information	833,600	0.3%	622,900	0.3%	3.8%
Multiple types	~	~	1,252,000	0.5%	7.6%
Existing account[b]	~	~	824,700	0.3	5.0
Other[c]	~	~	427,400	0.2	2.6

Note: Detail may not sum to total due to victims who reported multiple incidents of identity theft and rounding. See appendix table 1 for standard errors.

~Not applicable.

[a]Identity theft classified as a single type.

[b]Includes victims who experienced two or more of the following: unauthorized use of a credit card, bank account, or other existing account.

[c]Includes victims who experienced two or more of the following: unauthorized use of an existing account, misuse of personal information to open a new account, or misuse of personal information for other fraudulent purposes.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

TABLE 2

Persons age 16 or older who experienced at least one identity theft incident during the past 12 months, by victim characteristics, 2012

	Any identity theft		Misuse of existing credit card			Misuse of existing bank account			New account or personal information[a]	
Characteristic	Number of victims	Percent of all persons	Number of victims	Percent of all persons	Percent of persons with credit card	Number of victims	Percent of all persons	Percent of persons with bank account	Number of victims	Percent of all persons
Total	16,580,500	6.7%	7,698,500	3.1%	4.5%	7,470,700	3.0%	3.5%	1,864,100	0.8%
Sex										
Male	7,902,800	6.6%	3,932,000	3.3%	4.8%	3,320,100	2.8%	3.3%	851,200	0.7%
Female	8,677,700	6.9	3,766,400	3.0	4.3	4,150,600	3.3	3.8	1,012,900	0.8
Age										
16–17	35,200 !	0.4% !	4,300 !	0.1% !	0.7% !	16,300 !	0.2% !	0.6% !	5,800 !	0.1% !
18–24	1,466,400	4.8	331,400	1.1	2.6	937,400	3.1	4.1	182,400	0.6
25–34	3,293,500	7.8	1,177,500	2.8	4.1	1,718,100	4.1	4.7	406,700	1.0
35–49	4,914,800	8.0	2,222,100	3.6	4.8	2,344,600	3.8	4.3	531,900	0.9
50–64	4,739,400	7.8	2,590,400	4.2	5.4	1,853,300	3.0	3.3	501,500	0.8
65 or older	2,131,100	5.0	1,372,800	3.2	4.1	601,100	1.4	1.6	235,800	0.6
Race/Hispanic origin										
White[b]	12,417,600	7.3%	6,258,500	3.7%	4.9%	5,295,000	3.1%	3.4%	1,146,400	0.7%
Black[b]	1,494,100	5.0	301,400	1.0	2.1	896,300	3.0	4.2	361,500	1.2
Hispanic/Latino	1,544,100	5.2	509,100	1.7	3.1	834,300	2.8	3.8	254,000	0.8
Other race[b,c]	841,400	6.4	523,900	4.0	5.4	302,700	2.3	2.7	54,000	0.4
Two or more races[b]	270,700	9.0	102,000	3.4	5.9	133,400	4.4	5.3	48,200	1.6
Household income										
$24,999 or less	1,888,000	4.9%	413,200	1.1%	2.6%	1,068,800	2.8%	3.9%	419,400	1.1%
$25,000–$49,999	2,809,100	5.4	1,026,100	2.0	3.0	1,490,200	2.9	3.4	443,500	0.9
$50,000–$74,999	2,598,500	7.7	1,084,600	3.2	4.1	1,305,800	3.8	4.2	259,000	0.8
$75,000 or more	6,274,800	10.0	3,668,900	5.9	6.8	2,389,800	3.8	4.0	426,100	0.7
Unknown	3,010,100	5.1	1,505,700	2.6	3.7	1,216,200	2.1	2.4	316,100	0.5

Note: Estimates are based on the most recent identity theft incident. Includes successful and attempted identity theft in which the victim experienced no loss. See appendix table 2 for standard errors.

! Interpret with caution; estimate is based on 10 or fewer sample cases or coefficient of variation is greater than 50%.

[a]Includes the misuse of personal information to open a new account or to commit other fraud.

[b]Excludes persons of Hispanic or Latino origin.

[c]Includes persons identifying as American Indian, Alaska Native, Asian, Hawaiian, or other Pacific Islander.

Source: Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012.

their clients. Biometric technologies can verify a customer's identity based on unique characteristics, such as fingerprints, retinal identification, facial and voice patterns.

Financial institutions have been adopting the technology, mainly in the Asia-Pacific region, to strengthen their security infrastructure and to protect individual consumer banking profiles. While the U.S. situation outlined above describes the acute nature of the identity theft problem, biometrics in the North American banking sector have not yet been deployed on a wide scale for banking consumers. The reasons for this include the fact that both privacy expectations and considerations in Canada and the United States are quite different from those within emerging economies.

A recent article published by BiometricUpdate.com notes that while biometric authentication has been around for a while within the banking context, it has mainly been used to obtain voice authorizations from clients for banking services and for allowing banking employees to access facilities. However, in an effort to reduce risk from rampant identity fraud and theft, as identified above, financial institutions throughout North America are actively evaluating different biometric technologies.

The Biometrics Research Group projects that the implementation of new biometric technologies in the banking industry has the potential to cut a financial institution's operational risks by at least 20 percent over the next 10 years as the technology becomes more widely adopted.

With the advent of electronic banking, financial institutions are able to reach customers around the globe and conduct transnational business. However, in the process, financial institutions have experienced growth in exponential risk to their systems and processes.

Operational risks that financial institutions face are increasing due to the elimination of face-to-face service with the advent of electronic banking. Banks must verify the legitimacy of customer identifications, transactions, access and communications, which demands an incredible amount of vigilance.

Implementing a biometric-enabled authentication system can be a very efficient method of protecting the technological assets of an enterprise against the attacks of internal and external intruders.

Voice Biometrics

As a result of its accuracy, financial institutions have identified voice biometrics as one of the best means to secure its client accounts and financial information. Voice biometrics compares various characteristics drawn from a person's voice such as inflection, pitch, dialect, among others, and matches that with data captured. For voice recognition to work it requires banks and other financial institutions to register their clients voice patterns and correlate them to personal data for incorporation into a database.

Voice biometrics solutions allow customers to verify their identity simply by speaking, making it easier and faster to gain access to secure banking and insurance services by way of mobile apps, telephone and Web channels. Voice biometric solutions are popular because they eliminate the need for PIN-based password or interrogation-based authentication methods, or can be used to add another level of security to those systems.

Banks that deploy voice biometrics to automate the "log-in" process not only enhance customer satisfaction levels, but dramatically reduce their customer care costs through increased automation rates. In a typical scenario, a financial institution may allow a customer to reset a password over the telephone with voice recognition software that authenticates the customer. As a result, a number of large banks worldwide have explored the possibility of adding voice biometrics to enhance their customer roster this year. **JPMorgan Chase**, **Wells Fargo** and other large U.S. banks use voice screening to identify fraud suspects by listening for voices that match those from a database of fraud suspects.

U.S. Bank began piloting voice biometric software from **Nuance Communications** in early 2014. Under the pilot program, select credit card customers will use their voice to login with spoken passphrases to access account balances, search transactions and make a payment on their account in the mobile app. This most recent deployment comes on the heels of a partnership between U.S. Bank and Nuance in April 2013, which saw voice recognition used for conducting basic functions. The difference between these two systems obviously, is that one recognizes and verifies the identity of the user, while the other one does not.

As BiometricUpdate.com reported in November 2013, the **National Australia Bank (NAB)** has opted to use voice recognition for the biometric authentication of its customers rather than fingerprinting, as it reportedly deems the technology more secure and reliable.

The BiometricUpdate.com article notes that when customers call into to NAB's telephone banking call center, they have an opportunity to opt to use voice recognition. The recognition data is stored internally by the bank, and in order to ensure that recorded voice clips cannot be used to gain unauthorized access, the system uses a string of different questions that are difficult to "spoof".

Due to the versatility, along with consumer confidence in voice biometric technology, the Biometrics Research Group expects voice biometrics to be the fasting growing technology modality in the banking sector. Surveys we have analyzed have found that consumers prefer voice recognition technology for biometric identification.

According to a survey conducted by IT provider **Unisys**, the biometric modalities ranked by consumer preference are: voice recognition (32 percent), fingerprints (27 percent), facial scan (20 percent), hand geometry (12 percent), and iris scan (10 percent). As a result, the Biometrics Research Group projects that voice recognition will be widely adopted. We project the technology will not only be implemented in bank calling centers throughout the world, but fast growth will also be driven by the continued rapid worldwide adoption of mobile "smartphone" and "superphone" technologies.

Banks are in the preliminary stages of testing and rolling out new voice biometric technologies for mobile devices. In North America in 2013, **USAA**, the independent bank and insurance brokerage that caters to the U.S. military, developed a voice recognition service that will eventually allow its entire mobile phone customer base to make natural language inquiries for a wide range of banking services.

USAA's voice recognition app is currently being tested by a group of employees but is slated for use by the bank's 6.3 million account holders early next year. The bank has stated publicly that the application has tremendous potential to make banking: "simpler, faster and more satisfying on mobile devices."

The bank cites the fact that military personnel are often quite mobile and would like to make greater use of advanced smartphone and superphone technologies. The bank also cited statistics from its voice biometric technology supplier Nuance that while over 50 percent of smartphone and superphone owners have installed a mobile banking app on their device, only 27 percent actually use it on a regular basis. Consumers say improvements in a few areas would increase the use of smartphone and superphone banking apps significantly. Thirty-four percent say they would appreciate a seamless access to a live agent when they need one, and 21 percent want their mobile apps to include more self-service tasks. Eighteen percent would simply settle for an app that was easier to use.

Technology suppliers like Nuance are betting that voice biometrics will be the "magic sauce" that improves banking customer experiences. Other banks are also examining implementation of the voice

biometrics technology. Spanish bank **BBVA** is also currently developing a Siri-like banking application for iPhones and iPads at its U.S. subsidiary.

Further, in terms of timelines, major banks such as ANZ are seriously beginning to study implementing biometrics over the next three to five years to improve the quality of its banking services. **ANZ** has made public statements that it projects it will take two to three years before commercialization of biometrics in banking is achieved. However, the bank is positioning itself for the implementation of the new technologies, that will be designed to simplify ANZ's distribution networks and its products and processes, while providing customers with additional mobile and flexible banking options, while concurrently improving the capability of front-line staff.

Due to growing interest in providing consumers with cutting edge technology, while concurrently enhancing banking security, Biometrics Research Group expects more financial institutions to develop and deploy biometrics, and as a consequence, expects revenue growth for voice biometrics to grow. Our research estimates that at least US$200 million was spent on voice biometrics in the banking sector in 2012. **We estimate that at least US$750 million will be spent on voice biometrics in the banking sector by 2015.**

Use Case Study: AGNITiO Voice Biometric Solutions

One of the companies that Biometrics Research Group projects will benefit from voice biometrics growth in the banking sector will be **AGNITiO S.L.**

AGNITiO's solutions are geared for the banking sector because they provide strong authentication of telephone and electronic transactions. Unlike token-based one-time PIN generators, voice biometrics does not require the user to have any specific hardware, making the technology more economically suitable for mass-market applications. Users simply need access to a mobile or landline telephone. This makes voice biometrics a very suitable technology for phone and online banking, as well as many other corporate voice applications and security needs. Automated password reset procedures, presence monitoring, time and attendance, call center user verification and verification based on free speech are some examples of typical applications that can also be front-ended with AGNITiO's voice biometrics solutions.

AGNITiO Voice ID helps reduce financial services call center fraud. Between 75 and 95 percent of the cases detected are repeated attacks. Being able to spot the voices of those professional fraudsters can have a tremendous impact in fraud reduction. AGNITiO specializes in this detection.

AGNITiO Voice ID can also be deployed as part of the multi-factor authentication application. Such applications can increase access security without negatively impacting the customer experience. Authentication can be done in a remote server or locally in the device.

AGNITiO's KIVOX Mobile product is compatible with published security protocols, to guarantee secure authentication. Deploying Voice ID as part of a multi-factor authentication scheme also enabled financial services institutions to comply with the increasing number of government regulations, such as Federal Financial Institutions Examination Council (FFIEC) requirements in the United States.

KIVOX Mobile is a Software Development Kit (SDK) which enables on-device secure speaker verification of your own applications for smartphones and other embedded platforms. No network connection or voice transmission is needed to use this new secure method of mobile authentication. A user can be on an airplane and will be able to unlock his phone or protected files, simply by using his voice. Users can select a pre-defined passphrase

or choose their own to create a biometric voiceprint which can later be used for verification.

KIVOX also offers an API engine that provides some of the most advanced speaker authentication capabilities available in the market today. Their product enables mobile, Web, desktop or IVR voice applications to securely verify the identity of your customers in a highly secure, automatic and effortless manner. KIVOX 360 is optimized to work using a selected passphrase to create a biometric voiceprint which can later be used for authentication in any channel.

KIVOX Passive Detection is another API engine that provides 1:1 and 1:M Speaker Identification capabilities both in real time and offline. This API enables clients to implement passive authentication for call center customers while they are speaking with an agent. It also enables comparisons against a blacklist of up to 1,000 known fraudsters while a conversation is taking place, or as a batch process after the conversation has been completed. KIVOX Passive Detection offers the advantage of being fully text and language independent. The authentication process and blacklist comparison can be conducted in a fully transparent manner, without disturbing the customer or interrupting the flow of conversation. Such a system is of tremendous benefit within the "biometrics banking" space.

Biometric ATMs

As noted before, privacy concerns have prevented widespread deployment of biometric devices such as ATMs in North America. The use of ATMs throughout the developing world, however, is burgeoning, especially in Asia.

Automated Teller Machines (ATMs) that implement biometric technologies are an example of the use of a biometric identifier to authenticate consumers. Financial institutions that use such technologies can opt for biometric identifiers that either use a single or multi-factor authentication process.

Biometric ATMs are cash machines that use biometric measures to identify customers and allow them to withdraw cash. Biometric authentication may be the only customer identifier used, or it may be used in conjunction with another format, such as a payment card, a mobile device or an additional security credential, such as a personal identification number (PIN).

The biometric measures used in biometric ATMs generally include palm or finger vein print biometrics, although they may also include other functionalities such as iris recognition or face recognition.

Finger vein recognition is a method of biometric authentication that uses pattern recognition techniques based on images of human finger vein patterns beneath the skin's surface. Finger vein recognition is used to identify individuals and to verify their identity.

Finger vein recognition is a biometric authentication system that matches the vascular pattern in an individual's finger to previously obtained data. Hitachi developed and patented a finger vein identification system in 2005. The technology is mainly used for banking authentication and automated teller machines.

To obtain the pattern for the database record, an individual inserts a finger into an attester terminal containing a near-infrared light-emitting diode (LED) light and a monochrome charge-coupled device (CCD) camera. The hemoglobin in the blood absorbs near-infrared LED light, which makes the vein system appear as a dark pattern of lines. The camera records the image and the raw data is digitized and held in a database of registered images.

Blood vessel patterns are unique to each individual. Unlike other biometric systems however, blood vessel patterns are almost impossible to counterfeit because they are located beneath the skin's surface and can only be obtained from a living person.

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle. Before recognition of the iris takes place, the iris is located using landmark features. These landmark features and the distinct shape of the iris allow for imaging, feature isolation, and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (e.g., eyelashes, reflections, pupils, and eyelids) in the image may lead to poor performance. Iris imaging requires use of a high quality digital camera. Today's commercial iris cameras typically use infrared light to illuminate the iris without causing harm or discomfort to the subject.

Facial recognition systems are computer applications that automatically identify or verify a person from a digital image or a video frame from a video source. Methods for identification include comparing selected facial features from an image capture against a facial database.

These biometric identifiers are the key systems used in biometric ATMs. While most banks in North America have not yet ventured to use biometric ATM solutions to enhance their customer offerings due to social and legal issues, many other financial institutions in the emerging economies of Eastern Europe, Latin America, Asia and the Middle East, which are not restricted by law or behavioural customs have experimented with viable implementations of biometric-enabled authentication systems for their customers.

Banks in Japan have widely deployed biometrics-enabled ATMs that allow customers to withdraw currency or conduct other transactions after a successful fingerprint or finger vein scan. There are currently more than 80,000 biometrics-enabled ATMs in Japan and more than 15 million customers using them. Similar programs have been launched in China, Brazil and India.

In 2011, **Leto-bank**, a subsidiary of Russia's VTB, stated that it planned to deploy ATMs equipped with fingerprint scanners to authenticate its customers. And in Japan, Ogaki Kyoritsu Bank began to offer card-free ATMs that allow customers to withdraw cash, make deposits and check account balance by way of biometric palm scans.

In Poland, **Bank BPH S.A.**, committed to implementing finger vein biometrics authentication at its ATMs, providing its customers with more secure money transaction services without the need to use PINs to verify individuals. Subsequently, all of the nearly 300 of the Polish bank's branches will start using it as a main method of authentication at teller counters by this year.

Throughout Palestine and Jordan, **Cairo Amman Bank** has used biometrics to register 100,000 customers. The Middle Eastern-based bank has deployed over 500 iris cameras to verify customer transactions at all customer service desks, teller stations and ATMs.

In Latin America, **CAIXA**, Brazil's second largest bank, announced in the summer that it had opted to introduce fingerprint sensors to its ATMs. Likewise, in the summer, Brazilian international bank **Itautec**, also committed to deploying 12,000 automated banking machines with multispectral fingerprint readers.

The driving "push" factor for biometric ATM adoption is that biometric technology shortens transaction times. It also provides security unlike other measures in common use. Using biometric ATMs

can deter crimes like Internet banking fraud, money laundering, and identity theft and therefore are a popular option in Asian and emerging economies that have fewer cultural limits on the use of such technology.

Mobile Commerce

In terms of banking trends, Biometrics Research Group projects that mobile commerce will emerge as the next killer application for biometrics and the industry segment will be led by smartphone manufacturers such as Apple and by payment processors such as **PayPal**.

Previously, we accurately predicted that biometrics would become integrated within a wide number of mobile devices during the last smartphone product release cycle. The consultancy also correctly predicted that integration would be driven by smartphone and tablet manufacturers such as **Apple** and **Samsung Electronics**. Now, another prediction has proved 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 October 2014, BiometricUpdate.com reported that Apple had launched its "Apple Pay" app allowing customers to easily make retail payments through their mobile phones. The launch of the mobile wallet application was timed to coincide with the launch of the long-rumoured iPhone 6 in October. This time horizon allows Apple to build popularity and market share for the Apple Pay app on the lead-in to the holiday shopping season and the New Year. The new app leverages the firm's Touch ID fingerprint sensor within the new iPhone 6 and 6 Plus smartphones to verify a customer's identity.

The new iPhone includes a "secure element" system that allows it to store sensitive data such as financial credentials. This secure element system is the same secure system that currently stores the user's fingerprint data and has the ability to store future mobile health data. Apple is operating the system without giving up control to wireless carriers.

Apple partnered with credit card companies, financial institutions and retailers for the new payment service, along with major merchants including Walgreens, McDonald's, Macy's and Staples to introduce a NFC-powered mobile payment service.

Last year, the Biometrics Research Group predicted that worldwide mobile payment transactions would reach US$250 billion in 2014. The research consultancy, which publishes BiometricUpdate.com, also estimates that global annual transactions will hit US$750 billion by 2020, with more than 700 million consumers taking advantage of mobile payment systems.

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.

In a previous special report on mobile biometric authentication, the Biometrics Research Group predicted that the inclusion of biometrics in mobile devices will generate about US$9 billion worth of revenue for the biometrics industry by 2018.

According to Forrester Research, commerce transactions in the United States completed on mobile phones and tablets are expected to total US$114 billion in 2014. Two-thirds of those sales, or about US$76 billion, are occurring on tablet computers, while the remainder are occurring on mobile phones. This equals nearly a third, or 29 percent, of all e-commerce transactions that occur. While mobile commerce is growing quickly, currently it only accounts for nine percent of total commerce transactions in the U.S. By 2018, Forrester Research projects that mobile commerce will account for 11 percent of all commercial transaction. Also by 2018, Forrester expects that mobile commerce transactions in the U.S. will total US$414 billion.

A wide number of these transactions will be processed by PayPal. Currently, PayPal is one of the fastest-growing digital payment providers, with more than 152 million active registered accounts. Accounts grew 15 percent year-over-year last quarter. Revenue over the last 12 months grew by 19 percent over the prior year period to approximately US$7.2 billion.

According to the latest stats, PayPal facilitates one in every six dollars spent online today worldwide. Total payments volume over the last 12 months increased by 26 percent to US$203 billion, providing merchants and consumers worldwide a faster, safer way to pay and be paid.

The company also leads in the development of mobile payment technology, as it recently launched its "One Touch" mobile payments feature, that allows consumers with PayPal accounts to link those accounts to their mobile device in order to complete a purchase on that device with a single tap. Analysts suggest that a wider strategy might include leveraging wireless Near Field Communication (NFC) technology that is embedded into new iPhones, which effectively turns smartphones into payment tap devices that can used be at brick-and-mortar retail locations.

Such a system would evidently compete against the recently unveiled Apple Pay system though PayPal has officially stated that it sees room for multiple payment systems. PayPal however need not be cooperative with Apple due to its current market relationships and reach. PayPal is fully localized in 26 currencies, is available in 203 markets worldwide and has relationships with 15,000 financial institutions. Representative of its global reach, PayPal is the number one payments processor for business to consumer exports for Chinese merchants. These numbers demonstrate that smartphone manufacturers and payment processors will challenge traditional financial institutions such as banks and credit card payment processors for control of the mobile commerce marketplace. These companies will also be innovation drivers for the integration of NFC and biometric technology for real-time payment services.

Government-Driven Banking Initiatives

The other major, non-traditional player in the biometric banking space will be governments. Indeed, governments in emerging economies have rapidly been embracing biometric banking technologies for retail consumers for payment verification. According to numerous BiometricUpdate.com reports this year, growing assortments of countries have been using biometric technologies to verify recipients of government payments.

In the Philippines, the government has been using biometric technology to authenticate cash grant beneficiaries for poor households. In Pakistan, the government has begun to issue biometric smart cards to pensioners, enabling them to withdraw pensions from banks and post offices. But the most dramatic example of government-driven biometric banking is the Indian government's proposed use of Aadhaar to issue bank accounts to all Indian households.

Aadhaar is the world's largest biometric database. Recently, the Indian government allocated US$340 million to accelerate resident registration. The government's objective is now to enroll 100 million more residents with Aadhaar. UIDAI has already enrolled about 700 million. Currently governed by the Unique Identification Authority of India (UIDAI), Aadhaar is presently used to authenticate delivery of social services including school attendance, natural gas subsidies to India's rural poor, and direct wage payments to bank accounts.

The new Indian government under the direction of Prime Minister Narendra Modi has decided to expand the use of the Aadhaar system to help deliver even more welfare initiatives and programs, including Modi's new Pradhan Mantri Jan Dhan Yojana scheme. The new program, which means "Prime Minister Scheme for People's Wealth" aims to provide a bank account for each household in India. Financial Services Secretary G. S. Sandhu has described the scheme as an important step towards converting the Indian economy into a cashless and digital economy.

The new scheme is an expansion of an Aadhaar banking pilot project which the Indian government previously launched that is entitled "Saral Money". Saral Money is a unique financial services and electronic payments program that uses Aadhaar. In conjunction with Visa, five Indian banks have created a system to ensure that anyone with an Aadhaar number can be immediately issued a prepaid payment card.

Two-Factor Authentication

Biometrics Research Group, Inc. believes that the future of biometric technologies in the context of banking will be driven by two-factor authentication. Two-factor authentication involves the combination of at least two biometric modalities.

An authentication process that relies on a single biometric identifier may not work for everyone in a financial institution's customer base. Introducing a biometric method of authentication requires physical contact with each customer to initially capture the physical identifier. This process increases deployment costs. Unlike a password or PIN system, in which a financial institution needs to communicate with a customer only once for account initiation, use of biometric identifiers for authentication may require customers to submit several samples, sometimes over time. Some customers may not be able to produce a given biometric identifier, because of particular physical attributes or disabilities.

Even when the customer is able to produce a biometric identifier, there may be times when the biometric identifier cannot authenticate the customer. For example, if a customer has a severe cold, or laryngitis, voice recognition identifiers may mistakenly restrict the customer's access.

Financial institutions can eliminate this problem by allowing for more variation in the biometric sample input compared to the database, but this will reduce overall security and potentially increase the number of individuals that the system may falsely authenticate. As analysts at IDC have noted, banks should not stop using traditional passwords despite biometric identification measures. While a biometric identifier in theory could replace the personal identification number, a customer should instead be asked to supply a PIN or password to supplement a biometric identifier, making it part of a more secure two-factor authentication process.

The use of biometric identification technologies in financial applications is a "relatively young and experimental business," Andrei Charniauski, an analyst for IDC said. According to Charniauski, it will take "several years" for the financial sector to fully assess biometric technology safety levels. In the interim, however, IDC suggests that banks ought to provide two-factor authentication.

There is now advanced technology such as face and voice recognition biometrics to prevent account takeovers. Combining both face and voice of the account holder, ID theft becomes virtually impossible. According to some marketplace studies, the accuracy is around 99.9 percent. Due to this level of accuracy, Biometrics Research Group, Inc. notes that two-factor authentication will become a key approach to many biometric banking applications. Currently, some biometric ATM deployments in Japan utilize two-factor authentication whereby both palm print authentication is combined with passcode or PIN.

Palm print innovator **Fujitsu** has been the driving force for combined two-factor biometric authentication systems. In 2012, Fujitsu revealed the creation of the world's first biometric system that combines both palm vein recognition with fingerprint verification. By unifying the two biometric techniques, the firm has been able to develop a technology that is able to identify one individual from a million others, in less than two seconds.

According to the company, its system makes it possible to build authentication systems that do not need physical ID cards. Further, the system can be customized to accommodate specific applications, such as small-scale room access control to large-scale access systems across multiple locations. Most importantly, the system is compatible with existing palm vein authentication and fingerprint authentication systems and equipment that are already in use.

Fujitsu already is a leading developer and manufacturer of palm vein systems. The company released its first publicly-available software development kit for palm vein technology in 2006 and the firm has been a supplier of palm vein technology for Japanese banks since 2004.

Conclusion

Biometrics Research Group, Inc. notes that revenue streams for biometrics utilized in the global banking sector will rise from US$900 million in 2012 to US$1.8 billion by the end of 2015. This means that biometric revenue from banking sector constituted approximately 12 percent of the entire US$7 billion marketplace in 2012 and is projected to continue to constitute 12 percent of the market in 2015. Revenue will primarily be driven by adoption in emerging economies, but market and technological research will continue to be conducted in developed countries. The North American consumer will continue to demonstrate reluctance towards the implementation of these technologies, while emerging economies, especially Asian countries, will continue to adopt them. Surprising growth areas will include governments that will use their biometric identity programs to extend banking to their citizens and to biometric payment processors, who will leverage biometrics to enable mobile commerce in brick-and-mortar environments.

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.

WHAT TO EXPECT

EXHIBITION SPACE

27,000 SQM

EXPECTED NUMBER OF EXHIBITING COMPANIES

250

EXPECTED NUMBER OF TRADE VISITORS

8,000

450
KEY DECISION-MAKERS FROM INTERPOL'S

190
MEMBER COUNTRIES

Contact us TODAY at +65 6389 6614 or sales@interpol-world.com

Event Owner: INTERPOL

Supported By: Ministry of Home Affairs; Singapore Exhibition & Convention Bureau

Supporting Knowledge Partner: Frost & Sullivan

Held In: YourSingapore

Managed By: MP international