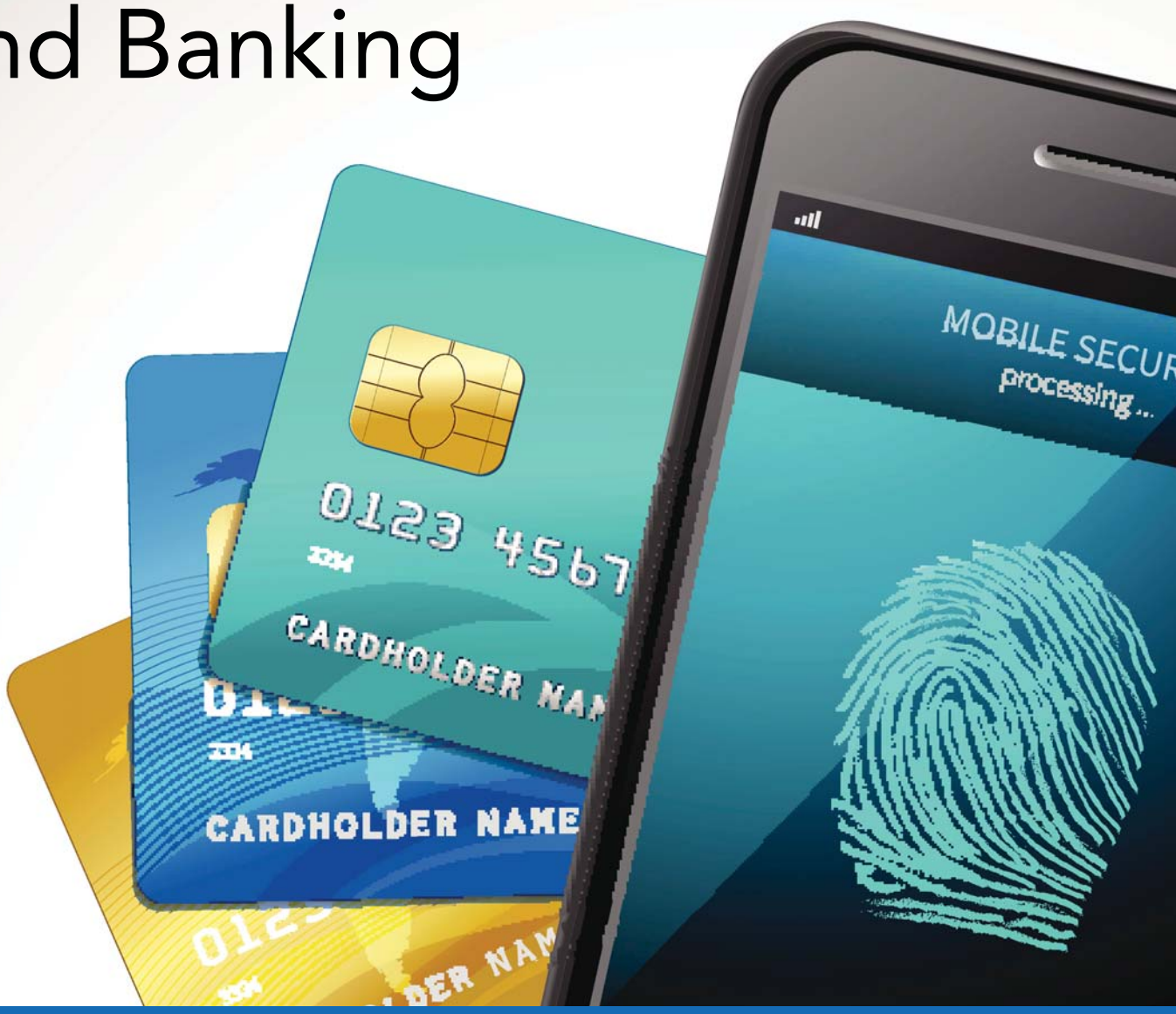
Biometrics and Banking



BIOMETRIC UPDATE.COM

This white paper provides an updated overview and market synopsis of biometrics for the global financial sector.

Rawlson O'Neil King Lead Researcher, Biometrics Research Group.

FINGERPRINT AUTHENTICATION FROM THE INSIDE OUT.

Utilizing Lumidigm's multispectral imaging, HID Biometrics is employing advanced technology to scan and authenticate fingerprints from the inside out. By capturing additional data from below the surface of the skin, we can read and match fingerprints even when the external characteristics are damaged or obscured. When it's important to know "who" is transacting, the only option is secure, convenient and trusted biometric solutions from HID Global.

You'll call it authenticating with confidence. We call it, *"your security connected."*

YOUR SECURITY. **CONNECTED** | Visit us at hidglobal.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 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.

Market Size and Synopsis

Biometrics Research Group, Inc. believes that the financial services sector has emerged as a primary end-user market for biometrics technology worldwide. We define 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, palms, gait, face or even voice.

Biometrics Research Group, Inc. estimated that total revenues for biometrics supplied to the global banking sector totaled US$900 million by the end of 2012. We subsequently projected that total revenues in the sector increased to US$1.8 billion by the end of 2015. This means that biometric revenue from the banking sector constituted approximately 12 percent of the entire US$7 billion marketplace in 2012 and is likewise projected to make up 12 percent of the market in 2015. By the end of 2016, we believe that revenue will continue to increase to US$2.2 billion and we further estimate that the financial biometrics market will eventually account for almost a third of total biometrics market revenues globally by 2020. Biometrics Research Group also projects that the market will grow at a compound annual growth rate (CAGR) of more than 50 percent from 2016 to 2020.

We believe that our projections are in line with other research vendors. Goode Intelligence predicts that the biometric market for financial services will reach a value of US$11 billion by the year 2020. Goode Intelligence also asserts that by 2020, there will be 622 million mobile banking applications offering biometric authentication, with US$5.6 trillion in payments secured by biometric technology.

Biometrics Research Group, Inc. believes 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. Although government and civil identity applications have been early adopters and the largest implementers of biometrics over the past decade, commercial and consumer sectors have become important target markets, especially in regards to financial services. The adoption of biometrics by the financial services sector can be attributed to the need to offset increased fraudulent activity and identity theft.

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 notes 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.

Major news sources reported in mid-2015 that 21.5 million people were affected by a breach of U.S. government systems. Identity data gathered over the last 15 years was compromised, including personal information about individuals who were part of government employee background checks. Unfortunately, even the best risk-based, multi-layered breach defense is imperfect, and incidents like this are inevitable. For this reason there must be greater focus on controlling what happens after the breach, including ensuring that stolen identities are unusable by anyone but their legitimate owners.

Ensuring Biometric Data is Useless to Identity Thieves

HID Global notes that biometrics is the only authentication method that binds a myriad of digital and physical credentials to a person. As such, biometrics plays an important role in eliminating digital identity theft in today's increasingly complex and vulnerable digital environment.

Fingerprint images were among the sensitive information that was stolen in the 2015 U.S. Office of Personnel Management (OPM) breach. Conceivably, this biometric data could be used by the perpetrators to hijack a user's identity and gain fraudulent access to security systems.

It is important to understand that biometric characteristics are not secrets. Facial characteristics are quite public — not only observable, but also generally associated with our names and other personal information. In the OPM example, now that fingerprints have been stolen from government databases and can never be taken back, the key question becomes what can or should be done to render this information useless to any would-be impostor? Given the premise that databases are inherently vulnerable to attack, the challenge is one of minimizing negative impacts of a breach on individuals and organizations.

As always, the answer depends on the use case, and each category of applications must be examined individually and its associated threats assessed. In this complex and interconnected digital world, systems must be thoughtfully designed and deployed in order to protect user identities and ensure appropriate levels of security within the context of the application.

In the case of biometric data that is already "in the wild" (such as that stolen from the OPM), numerous tactics and best practices should be considered in order to render identities useless to anyone but the legitimate owner. Of critical importance is the ability to detect fraudulent attempts to use biometric data. Liveness detection — the real-time determination that the biometric characteristics presented are genuine and not fake — is a highly effective design feature in solutions where users physically interact with authentication systems.

Augmenting biometric liveness detection with other security layers for multi-factor authentication greatly enhances digital security and

renders the theft of any one personal data element inconsequential. There are also a number of concepts that combine biometric data and other data elements to create an even more robust digital credential that will ensure stolen biometric data is insufficient and therefore useless in enabling the fraudulent use of legitimate identities.

Following are the key elements in a strategy that extends beyond breach defense to include tactics for neutralizing the effects of an identity breach after it has happened.

Improving Liveness Detection

HID Global notes that one of the most effective liveness detection approaches for fingerprint biometrics uses Lumidigm® multispectral imaging technology, which virtually eliminates the possibility of counterfeit fingerprints being used for authentication. The technology is used to compare the complex optical characteristics of the material being presented against known characteristics of living skin. This unique capability, in addition to the collection of unique fingerprint characteristics from both the surface and subsurface of the finger, results in superior and reliable matching performance paired with the exceptional ability to detect whether the finger is alive or not. Multispectral imaging sensors are different from competitive offerings in that they:

- Use multiple sources and types of light along with advanced polarization techniques to capture information from the surface and subsurface of the finger — all the way down to capillary beds and other sub-dermal structures;

- Utilize advanced machine learning algorithms that can be updated in the field as new threats and spoofs are identified, enabling the sensors to very quickly respond and adapt to new vulnerabilities.

Multi-Factor and Multi-Modal Authentication

For strong and reliable user authentication, organizations should consider, where practical, multi-factor and even multi-modal authentication. Today's authentication technologies enable solutions that can enhance security while replacing passwords and improving convenience in a seamless way that is non-intrusive to the legitimate user.

For example, personal devices like smartphones, wearables, RFID cards and other intelligent personal devices can all generally be used as factors of authentication. Regardless of which additional authentication factor is presented by the user, when it is intelligently combined with biometric data associated with an identity claim, it is possible to quickly determine a definitive "yes" or "no". Strong authentication by means of two or more factors (with one being a biometric) is fundamentally more secure than outdated username/password alternatives.

When identity is firmly established, the use of mobile devices in authentication solutions offers the opportunity for greater personalization and a seamless experience for legitimate users. Information systems can be tailored to each user's need, resulting in enhanced, individualized security, allowing individuals to fully control their real identity. Instead of the system blocking the legitimate user — an unintended consequence of blocking an attacker — the system is made more secure and efficient and thus returns a higher ROI for both the consumer and system administrator.

More Robust Biometric Templates

It may be desirable in some application-dependent situations to construct and enforce the use of enhanced biometric templates. The use of a "super template" that uniquely combines biometric data with other information — perhaps even an OTP or other out-of-band data — enables the system to recognize and reject a biometric template that was created from a stolen fingerprint image. Templates can reside on a card or chip or in a smartphone or personal wearable.

In the case of a government or civil application, this approach would prevent any would-be attacker from simply using the stolen biometric data, alone, to compromise either physical or data security.

In the case of commercial markets (e.g., a banking application), we might see an institution deploying a similar approach to protect user identity during online transactions. As some do today, institutions could enable multi-factor authentication and require that both the biometric and some other data be provided. Alternatively, they could enroll biometric data and then "sign and encrypt" the template with unique or closed-system data.

The creation of a guaranteed unique "super template" might combine standard (interoperable) and proprietary data. This is the approach that HID Global takes with its Secure Identity Object™ (SIO), which is a data model for storing and transporting identity information in a single object. SIOs can be deployed in any number of form factors including contactless and contact smart cards, smartphones and USB tokens, and ensure that any of these items and the data associated with them are, in turn, only associated with the owner's identity. The SIO is digitally signed using proven cryptographic techniques as part of a seamless and secure process. Various data objects can be added, encrypted, and signed, i.e., biometric data, as well as data for computer log-on and other secure identity applications. Then, all content is secured with a wrapper and bound to the device with another signature.

Identity Proofing

Lastly, it's important to remember that the chain of trust is only as strong as the weakest link. The biometric solution used in identity-proofing must interoperate with trusted devices at each verification point. An example of this approach is HID Global's Seos™-based solutions, which create a device-independent, trusted physical identity verification process. Additionally, the physical devices themselves must be tamper-resistant to ensure that all transaction integrity is preserved. The HID Global Lumidigm biometric authenticator is a good example of this approach:

- Trusted devices must be encryption-enabled with various tamper resistance and detection capabilities that protect the integrity of the communication between the client and the sensor.

- The chain of trust must be preserved end-to-end if the goal is -- for example -- to simplify financial transactions for users while eliminating fraud for financial institutions.

- The end-point device must connect to the institution's systems through a cryptographically secure channel protected by hardware tamper detection and response, which establishes trust between the device and the institution's systems independent of intermediate systems and networks.

- A trusted biometric device must be able to perform a live scan of a finger with strong liveness detection to ensure that the person making the transaction is who they claim to be (that is, the same person that enrolled their biometric fingerprint).

And finally, by extension, if a card, smartphone, PIN, or other authentication factor is used for authentication, each must also be confirmed by a biometric — a biometric that is associated with a specific individual through a robust identity-proofing process at enrollment. This ensures that true identity verification has been performed and maintained in a trusted manner.

Moving Forward

Biometrics solutions offer the ideal balance of convenience and security because they are simple to use and increasingly more robust and reliable. Biometrics is also the only authentication method that "binds" a user's digital credentials to a person. As such, biometrics is playing an important role in eliminating digital identity theft in today's increasingly complex and vulnerable environment.

Making security more robust and reliable without adding complexity is difficult. But as our networks become more available and open to attacks, we simply have to find a way to enhance both trust and user convenience. Combining the universality and sophistication of biometrics with things we have (like personal devices, phones, wearables, etc.) and things we know (like PINs or passwords) is one important step. The other is to rely on vendor technologies and solutions that can effectively guarantee a high level of trust without raising the complexity for the user.

Wide Adoption of Biometrics in Payments

Due to the multiplicity 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 their clients. In one of their latest reports, Goode Intelligence expects that biometrics will eventually replace personal identification numbers (PINs) for automated teller machine (ATM) security in different scenarios. Goode Intelligence also expects payment solutions to support biometric modalities that are compatible with wearable devices, thereby leveraging heart rate, behavioral and multimodal biometric authentication. The firm claims that there will also be expansion in contactless mobile payments, using solutions offered by Apple, Google, Samsung, PayPal, Alipay and traditional payment scheme providers. Goode Intelligence further expects an increasing occurrence of card-not-present fraud combated by mobile biometric user authentication and step-up transaction verification.

The wide adoption of mobile devices with integrated biometric functionality ensures the use of the technology to secure transactions. Biometrics Research Group predicted that worldwide mobile payment transactions would reach US$250 billion in 2014. Our research consultancy 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.

Biometrics, which verify an individual's identity based on their unique physiological and behavioral characteristics, offer advantages of enhanced security, convenience, and time efficiency, which benefit financial institutions. Concurrently, the technology also offers consumers protection and peace of mind, which is important as mobile computing and commerce become more prominent components of the

consumer landscape. Mobile payment transaction growth, combined with biometrics, ensures 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 terms of banking trends, Biometrics Research Group, Inc. 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 payment processors like as PayPal.

Previously, Biometrics Research Group 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 like 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-rumored 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.

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, e-commerce transactions completed on mobile phones and tablets in the United States was expected to total US$114 billion in 2014. Two-thirds of those sales, or about US$76 billion, had occurred on tablet computers, while the remainder are occurring on mobile phones. This equals nearly one third, or 29 percent, of all e-commerce transactions that occurred. 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 transactions. 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 statistics, 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, which 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, 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.

Traditional payment processors are also benefiting from biometric integration. Mastercard reported that Dutch participants of its first worldwide biometric pilot embraced biometrics-based payment technology. Ninety-five percent of fingerprint users and 80 percent of the facial recognition users indicated that shopping became more convenient using biometric authentication. Seventy-five percent of users were convinced that biometrics-based payments will decrease fraud.

Regulations to Drive Financial Biometrics Market

Analysis from Biometrics Research Group notes that regulations will drive continued growth in the financial biometrics market.

In North America and Europe, regulatory compliance continue to be main motivations for financial institutions to adopt biometrics. Prominent government regulations include: the Federal Financial Institutions Examination Council (FFIEC) guidelines, the Sarbanes-Oxley Act of 2002 and the Basel II Accord.

Regulatory activity has resulted in increased demand for secure authentication of banking accounts, stronger employee audit trails as well as risk mitigation. Although the regulations do not endorse any specific technology, biometrics is emerging as the favored choice, owing to its capability of being able to accurately link any transaction with an individual's unique traits. While the technology can benefit consumers by more securely protecting their confidential data, biometrics can also reduce operational risks.

Biometrics Research Group, Inc. 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 and 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.

In terms of banking customers, a biometric identifier can measure an individual's unique physical characteristic or behavior and compare it to a stored digital template to authenticate that individual. Biometric identifiers can be created from sources such as a customer's voice, fingerprints, hand or face geometry, the iris or retina in an eye, or the way a customer signs a document or enters keyboard strokes. All of these identifiers are used in the banking sector, in a myriad of ways. Customer voice recognition is used by call centers and phone call verification systems. Fingerprint, hand and face geometry are used by automated teller machines (ATMs). Signature verification is increasingly being used for cheque verification. Keyboard stroke identification is also being used for online user verification.

Financial institutions have also taken to combining multiple authentication factors. Multi-factor authentication is a method of multi-faceted access control which a user can pass by successfully presenting authentication factors from at least two of the three categories:

- knowledge factors ("things only the user knows"), such as passwords or passcodes;
- possession factors ("things only the user has"), such as ATM cards or hardware tokens; and
- inherence factors ("things only the user is"), such as biometrics

Knowledge factors are the most commonly used form of authentication. In this form, the user is required to prove knowledge of a secret in order to authenticate, such as a password. A password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many multi-factor authentication techniques rely on password as one factor of authentication. Variations include both longer ones formed from multiple words (a passphrase) and the shorter, purely numeric, personal identification number (PIN) commonly used for ATM access.

Many security questions such as "Where were you born?," are poor examples of a knowledge factor because they may be known to a wide group of people, or be able to be researched.

Possession factors include both connected and disconnected tokens. Connected tokens are devices that are physically connected to the computer to be used and transmit data automatically. There are a number of different types, including card readers, wireless tags and USB tokens. Disconnected tokens have no connections to the client computer. They typically use a built-in screen to display generated authentication data, which is manually typed in by a user. Factors that are usually associated with the user include biometric methods, including fingerprint readers, retina scanners or voice recognition.

Requiring more than one independent factor increases the difficulty of providing false credentials. Two-factor authentication requires the use of two of three independent authentication factors, as identified above. The number and the independence of factors is important, since more independent factors imply higher probabilities that the bearer of the identity credential actually does hold that identity.

Multi-factor authentication is sometimes confused with “strong authentication.” However, “strong authentication” and “multi-factor authentication”, are fundamentally different processes. To clarify, strong authentication has been described as any method of verifying the identity of a user or device that is intrinsically stringent enough to ensure the security of the system it protects by withstanding any attacks it is likely to encounter.

Strong authentication is a commonly used term that is largely without a standardized definition. According to the European Central Bank (and the many organizations that follow its guidelines), strong authentication combines at least two mutually independent factors so that the compromise of one method should not lead to the compromise of the second. Typically, the authentication method must include one non-reusable element, which cannot easily be reproduced or stolen from the Internet. The term strong authentication is often used synonymously with two-factor authentication (2FA) or multi-factor authentication (MFA). However, that usage is misleading because some types of very secure authentication rely on a single authentication factor. Soliciting multiple answers to challenge questions can typically be considered strong authentication, but, unless the process also retrieves “something the user has” or “something the user is”, it is not considered multi-factor authentication.

The combined use of multiple factors allow financial institutions to combat identity theft and bank fraud by increasing overall security and by reducing the potential for users to be falsely authenticated. As many research analysts have noted, banks can augment traditional passwords or passcodes with two-factor authentication measures that include 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. Some banks in Asia currently leverage biometric identifiers such as finger vein and palm print recognition, in conjunction with ATM cards to provide an innovative, two-factor ATM authentication solution to their clientele.

Further innovative biometric solutions are being deployed in developing regions of the world, including South Asia, Latin America, and Africa, in order to reach vast rural populations. This segment of the population has been largely underserved by the financial services industry due to illiteracy and distance from bank branches.

ATMs integrated with biometric sensors are growing in popularity, especially in developing nations. Since 2004, Columbia based Bancafe Bank has deployed hundreds of non-AFIS fingerprint-enabled biometric ATMs in rural Columbian towns to cater to coffee growers. Similarly, in 2006 in India, Citibank launched a non-AFIS fingerprint-enabled ATM to allow its microfinance customers to access funds sanctioned to them. The technology allows customers to withdraw funds using just their fingerprints rather than having to carry an ATM card.

In the medium term, biometrically-enabled ATMs can be used for more unique applications. There is significant potential for relief organizations to disperse aid through biometrically-enabled kiosks and ATMs. This will ensure that only the rightful recipients can access these funds.

The Only Summit Dedicated to the Integration of Biometrics in the Banking and Financial Services Industry

BIOMETRICS

in Banking & Financial Services

Ensuring Customer Satisfaction and Enhancing Security Through Cutting-Edge Technology

June 27-29, 2016 // New York, NY

Why You Can't Miss This Event!

- Develop a business case for your boss using the statistics from case studies **addressing consumer demands**
- Gain an in depth understanding of the strategies available to **implement voice biometrics** in order to **increase customer experience** in call center operations
- Learn how to improve your ability to maintain customer numbers and protect your customer's information by utilizing and integrating the technology into **mobile devices, online service applications,** and **ATM machines**
- **Streamline the mobile login process** by addressing security and payment authentication to ensure that the data is protected and how iris technology can advance the system

Biometric Update subscribers receive **20% discount** off standard rates with promo code: **BBF_BU**

Contact Us Today!

Sponsorship/Exhibit Information:
Brittany Hicks
P: 212-885-2756
E: Brittany.Hicks@iqpc.com

Attendee Information:
Maricarmen Gonzales
P: 212-885-2678
E: Maricarmen.Gonzales@iqpc.com

www.BiometricsBankingFinance.com

Identifying Parties to Electronic Banking Transactions

As HID Global Corporation has noted in a previous white paper, it is important to know who is actually engaging in transactions. Determining who is involved in transactions however has become more complicated in recent years for the banking industry. A typical bank customer in the developed world visits an ATM a few times a week and only rarely pays a visit to a human teller. In today's anonymous landscape, how does the bank know who is transacting?

More and more often at banks around the world, the answer is fingerprint authentication. Unlike other forms of strong authentication such as cards and PINs, biometrics is the only means of determining "who" is using the system. And with the introduction of Lumidigm® multispectral imaging, biometrics can solve the transactional security question while bringing user convenience to the table.

What does multispectral imaging have to do with it? The promise of biometrics — worry-free authentication performance as seen in the lab — was not fully realized in the field for many years because conventional biometrics technologies rely on unobstructed and complete contact between the fingerprint and the sensor. In the real world, dry fingers or a dusty sensor can interfere with the finger/platen contact requirements of conventional fingerprint sensors.

Multispectral imaging isn't as fussy. This more-effective technology uses multiple spectrums of light and advanced polarization techniques to extract unique fingerprint characteristics from both the surface of the skin and the subsurface, where fingerprint ridges have their foundation. Unlike surface fingerprint characteristics, which can be obscured during imaging by moisture, dirt or wear, the "inner fingerprint" lies undisturbed and unaltered beneath the surface. When surface fingerprint information is combined with subsurface fingerprint information and reassembled in an intelligent and integrated manner, the results are more consistent, more inclusive and more tamper resistant.

Fast forwarding to today, we now see a growing number of banks worldwide deploying multispectral imaging biometric authentication as both a retrofit to existing ATMs or as part of their next generation ATM rollouts. Not only do these solutions provide a definitive answer to the question "Who is transacting?" but they offer bank customers a fast and easy way to conduct their business.

Latin America Leading the Way

With its highly advanced financial systems technology, Latin America is embracing fingerprint technology for their ATMs. What started out as a security project has ended up being a product differentiator that attracts customers: banks enhance security with biometric authentication while offering their customers the convenience of doing all those things people would like to do at the ATM, unencumbered by remembering a PIN or even a card.

The Bolsa Família Program, which provides payments to low income families in Brazil to help keep their children in school, was the catalyst for using fingerprint biometrics to replace individual PIN numbers for access to Brazil's second largest state-owned bank, Caixa Econômica Federal (CAIXA). Many users in the program do not have bank accounts and use the ATM only once a month to get their stipend. As such, they often forgot their passwords and bank managers were spending too much time

resolving getting PINs renewed or changed. With 14,000 ATMs involved in the program and many millions of registered customers, this was a major problem.

Diebold ATMs with multispectral fingerprint readers replaced the PINs that bank customers historically used to authenticate their identity and access their accounts. CAIXA customers now simply insert their card and use a fingerprint reader to withdraw funds from the ATM.

The "Beach Program"

One of Latin America's largest private banks has deployed 27,000 ATMs enabled with Lumidigm fingerprint authentication. The multinational bank had concerns that multiple identities were being employed by some people within their banking system. The organization needed a way to insure that each person had only one identity and to provide all customers with convenient access to their accounts. Biometrics would solve both challenges.

The bank initially deployed multi-factor authentication, having their customers use bank cards plus a finger to authenticate a transaction at the ATM. In an effort to make banking services as convenient as possible for its customers, the bank also piloted cardless transactions. Limited value transactions were made available to customers who keyed in a portion of their account number and pressed their finger to the sensor.

Billed as the "Beach Program", the bank's customers could leave their wallets at home when they went to the beach or to a nightclub and still have access to cash. The pilot program was so successful that today the bank has expanded the cardless authentication option to all customers at all ATMs. Their finger is their wallet — the ultimate in banking convenience.

Clearly, high reliability is critical in this type of program. Additionally, ATM use is not typically supervised; there may not be a person on hand for customers to consult if there is a problem with a transaction. Because multispectral imaging technology provides good reads on the first try by viewing the surface and subsurface of fingerprints in any condition, fingerprint readers using the technology were chosen for the ATMs.

Biometrics Beyond ATMs in Banking

In markets where an ATM infrastructure may not yet be established, a biometric handheld device is used to authenticate both user and service provider to ensure proper delivery of service and provide a complete non-repudiated audit trail of those transactions. In India, the government has been diligently working for decades to find ways of providing services to the citizens of an entire sub-continent and, likewise, commercial entities also want to reach out to the poor, especially those who have been previously excluded because of the limited capability of conventional biometrics technology. With those goals in mind, long-term initiatives related to Financial Inclusion and Public Distribution systems have turned to biometrics as a means of securing field transactions and ensuring that citizens are protected and government services are being provided to those who are authorized to receive those benefits.

Thus, besides multispectral imaging sensors used in biometric ATMs, they are also deployed in handhelds that act like micro ATMs in applications where banking services — such as opening savings accounts, transferring funds, making deposits, withdrawing cash and obtaining loans — are taken to remote rural areas where citizens have no access to banks.

These fingerprint sensors guarantee that rural employment beneficiaries are actually the ones to withdraw their weekly wages. Other multispectral imaging-based handhelds are being used in public distribution systems and education projects, where the biometric is used by citizens for collecting rations and for the authentication of students' attendance reporting.

Preventing Identity Fraud

Biometric authentication reliably answers the question, "Who is transacting?" and provides added convenience to the end customer. But is it secure? Multispectral imaging sensors also incorporate best-in-class liveness detection. The technology's subsurface capability allows the sensors to evaluate the spectral qualities of the finger presented — and if it is a fake, it's rejected. Also available are encryption solutions to prevent man-in-the-middle attacks and tamper-resistant devices that self-destruct when opened.

Liveness detection capabilities are never more important than in South Africa, where concern over fraud and identity theft has grown to level where a banking risk information center (SABRIC) requires banks to take active measures to become "safe, secure and risk free." Fully-deployed biometric systems throughout the country are now meeting that goal. Today, multispectral imaging biometrics is deployed in the largest banks in South Africa at teller windows and is being piloted in ATMs.

Reliable, Convenient, Secure and Proven

Multispectral imaging biometrics has been successfully deployed at banks and ATMs for several years now. The technology is proven; the applications are varied. Does your bank want to find ways to improve transactional security? What form of authentication will provide them with identity assurance, convenience and a compelling ROI? Do customers prefer the increased convenience — and security — of using their finger instead of remembering their PIN or bringing their card to the bank? Customers already using biometrics at their ATMs insist that they prefer their fingers over PINs and cards.

Diverse Use of Biometric Modalities

A unique proposition of biometrics is the diverse number of modalities that find application in financial services. Modalities ranging from non-AFIS fingerprint recognition, face, iris, vein, voice, signature, and hand geometry recognition have all found varying levels of acceptance. The following chart depicts how various modalities are being utilized across the three major financial biometrics applications— Physical access control, logical access control, and transactional authentication.

In 2006, non-AFIS fingerprint recognition was a dominant modality. The technology's key strengths are its cost efficiency and high accuracy. It also has wide applicability in physical access control, logical access control, as well as transactional authentication. Non-AFIS fingerprint recognition technology is found across financial institutions for uses ranging from ATMs, access to bank vaults, and business PCs.

Other emerging biometrics such as voice verification and vein recognition are gaining traction globally. A number of banks in Europe have deployed voice verification technology to enable remote authentication of customers for telephone banking. In 2006, Netherlands-based

ABN AMRO deployed a telephone-banking customer verification solution utilizing voice biometrics in its contact centers. This installation is considered to be one of the largest deployments of biometrics in the financial services vertical.

Vein recognition that includes palm and finger vein recognition was largely prevalent in Japan and South Korea until 2005. After 2007, it began to emerge as a popular alternative to non-AFIS fingerprint recognition, especially for biometrically-enabled ATMs and increasingly for physical access control.

Despite vein recognition's high cost compared to non-AFIS fingerprint recognition, its contactless interface, low failure-to-enroll rate, and lack of association with criminal activity places the technology in a strong growth position. At present, vein recognition is in an early adoption phase, but has the potential to become a widely deployed solution as its price is anticipated to decline in the medium to long term.

Future Trends and Strategic Recommendations

Most financial institutions have adopted biometrics for operational and employee-facing applications. Wider deployment in the financial industry is anticipated as the number of successful credible reference sites increases and financial institutions realize the cost-efficiencies and benefits of biometric technologies in comparison to alternate security technologies.

From an end-user perspective, it is imperative to publicize the benefits that biometrics can offer in terms of convenience, cost efficiencies and time efficiencies.

With biometrics, the ability of financial institutions to provide more value to their customers, while complying with regulations, can provide them with a competitive advantage. Our bottom line: Biometrics is the only technology that assures identity and knowing "who" to a high degree of certainty. Biometrics is also unique in its ability to raise the bar on security while adding convenience for the end user.