BIOMETRICS
IN BANKING
THE FUTURE OF BANKING & FINANCIAL SERVICES

BAYOMETRIC
JANUARY 24, 2017

Written & Compiled By
Danny Thakkar
CEO & Co-Founder
Banks are losing staggering amounts of money in fraudulent transactions and other cybercrimes, almost $450 billion annually.
BAYOMETRIC

INTRODUCTION
Traditional security mechanisms like passwords, PINs or tokens are no longer considered sufficient and look very weak in the face of sophisticated intruder attacks. In today’s digital world, customers are increasingly using the internet for conducting a lot of financial transactions through their desktops as well as mobile. Thus, customers now have to manage more passwords and PINs which creates frustration and dissatisfaction. Also, passwords or PINs can be easily stolen. Thus banks and financial institutions need a very strong security mechanism which is reliable and accurate to protect customer’s money and build trust.

Biometrics is a strong authentication mechanism that is able to provide an added layer of security to banking and financial transactions. Biometric identifiers are based on the intrinsic characteristics of the individual such as fingerprint, palm vein, iris scan and hence are extremely difficult to fake under normal conditions. This is what makes them ideal for securing banking and financial transactions.

Financial institutions realize the need for this added protection and hence the financial biometrics market is showing an upward trend. According to research firm Tractica, the global biometrics finance revenue is expected to reach $2.2 billion by 2024.

FACTORS DRIVING THE ADOPTION OF BIOMETRICS IN THE BANKING AND FINANCIAL SERVICES SECTOR
One of the major factors leading to the adoption of biometrics in the banking and financial services sector is the need to combat the increasing instances of identity thefts and fraudulent transactions. Banks are losing staggering amounts of money in fraudulent transactions and other cybercrimes, almost $450 billion annually according to the Center for Strategic and International Studies. The scale of the fraud issue is so large that banks are keen on investing in stronger methods of authentication. It is estimated that biometric technologies will be able to reduce the operational risks of financial institutions by almost 20 percent in the next 10 years.

The average banking customer is now significantly aware of online threats and realises that passwords and PINs can no longer provide the required protection against sophisticated bank frauds. Thus their security preferences have shifted and they want stronger security solutions such as biometrics. Lengthy passwords are difficult to remember and not a secured access method as is evident from the large number of recent password hacks. Biometric solutions such as fingerprint recognition enable the customers to authenticate transactions with a swipe of their...
BIOMETRIC

fingerprint and hence are more convenient, secure and preferable.

Another major factor fuelling the implementation of biometric technology in the banking and financial services sector is the increasing use of mobile devices for performing financial transactions. The first biometric-enabled smartphone was introduced by Apple in September 2013. Touch ID is a fingerprint recognition feature in Apple mobile phone’s which enables customers to unlock devices and authenticate purchases from iTunes and other third party apps using their fingerprint. Other mobile manufacturers are also following suit and integrating fingerprint scanners into their mobile devices. Samsung, for example has linked its users to mobile financial services through PayPal and the users can authenticate transactions using their phone’s fingerprint scanner.

The addition of fingerprint readers to mobile devices for authenticating banking apps is helping to increase consumer acceptance of biometric security. It not only adds a very high degree of security to financial transactions but also a lot of convenience. The smart phone stores the user’s financial data securely and the users are freed from the hassle of remembering passwords or tokens to access their banking or payment applications. Thus the most compelling reason for the adoption of biometric technology in the financial services sector is its potential to reduce the incidents of fraudulent financial transactions and the cost savings arising from it.

Biometrics is based on the paradigm that the individual himself is the authenticating factor as opposed to what he knows (e.g. a password) or what he possesses (e.g. a swipe card). Biometrics such as fingerprint, iris scan or voice recognition is a much more reliable and accurate method of authentication. In the case of mobile banking, fingerprint authentication is much faster that typing a password or PIN making it highly convenient for users. The principles of reliability and accuracy along with convenience make the adoption of biometrics a very attractive prospective in the financial services industry.

BIOMETRIC MODALITIES THAT ARE USED IN FINANCIAL SERVICES INDUSTRY

There are several biometric modalities to authenticate banking customers as well as employees. The biometric modalities currently available for authenticating users are fingerprint identification, voice authentication, facial recognition and iris recognition.

Fingerprint identification: The most popular and recognizable biometric modality in the financial services sector is undoubtedly fingerprint recognition. Apple’s Touch ID has familiarized customers with fingerprint identification technology and has paved the way for other manufactures to follow suit. As
BIOMETRICS

fingerprint identification becomes the norm, customers look for similar convenience in authentication of financial transactions. Thus in the last couple of years, fingerprint identification has been integrated in banking apps and several banks such as Bank of America, JP Morgan Chase etc. now offer fingerprint authentication. Bank of America customers can save their fingerprints on mobile devices and use them to access their accounts thereby completely eliminating the need of passcodes.

**Voice authentication:** Bank customers find it highly inconvenient to punch in a long account number or answer a series of tedious questions each time they access phone banking services. While this process is simply the bank’s way of ensuring that the person who called is actually who they claim to be, it might be quite annoying and frustrating for the customer. The solution to this lies in voice authentication biometrics. The customer’s voice is first registered into the system. Later when the customer calls phone banking, his or her voice is matched against the stored data and the matching can be completed in a few seconds. Many large banks such as Citi are testing voice authentication and looking to integrate this biometric technology in their banking services.

**Facial recognition:** Mobile customers can use their smartphone cameras to take a photo of their face and use it for approving online purchases. MasterCard recently rolled out a new payment technology application called Identity Check Mobile in the European Market. MasterCard holders can use either fingerprints or facial recognition to verify their identity. Typical payment authentication methods require the customer to remember and enter a password. If the customer enters a wrong password the transaction might be declined. Hence current methods are time consuming and cumbersome for the users.

With Identity Check Mobile, customers can either use fingerprint recognition or facial recognition technology to authenticate themselves. With facial recognition technology, they can take a ‘selfie’ photo using their phone’s camera and authenticate themselves to the online payment application. This marks a significant milestone in mobile payments through the use of biometric technology.

**Image 2: Bank ATM Recognition By Iris**

**Iris Scan:** Withdrawing cash from ATM using a magnetic stripe card is a 50 year old technology. The next generation ATM comes equipped with iris scanners. Though it is a relatively new innovation, Citibank and Diebold tested ATMs with iris scanners last fall in New York. Unlike traditional ATMs, these new-generation ATMs do not have a number pad or a screen.
**BAYOMETRIC**

The user enters the dollar amount in his or her mobile app to set up a transaction. Later, in the ATM he or she places his eye near the iris scanner which records a quick video and matches it with his previously registered scan in the system. The ATM machine will dispense cash on a positive match. Iris scanning technology validates the liveness of a person with the help of infrared light and hence it is impossible to trick this system with a picture, a video or even a disembodied eyeball.

**HOW IS BIOMETRICS USED IN THE FINANCIAL SERVICES SECTOR?**

Biometrics as an authentication technology has the versatility to secure transactions as well as provide a high degree of accuracy irrespective of whether the transactions are done through a smartphone, internet banking, ATMs or at bank branches. The adoption of biometrics in the banking and financial services sector will provide numerous benefits and eliminate the loopholes of traditional security mechanisms.

In branch banking, fingerprint scanners at the counter provide fast and accurate authentication for bank customers. The customer simply needs to swipe his finger at the counter and the fingerprint reader matches it with the customer’s existing template in the bank database. A successful authentication will allow the customer to continue with his financial transactions. This system is highly accurate and difficult to spoof as the identification factor is part of the customer’s inherent being. Also, it helps to maintain a concrete audit trail of each transaction thereby preventing the occurrence of any fraudulent activity.

**Image 3: Internet Banking**

Internet banking provides the flexibility of performing financial transactions from anywhere in the world using a laptop, computer or a mobile phone. This flexibility also brings a lot of vulnerability to such transactions and strong authentication methods are needed to maintain the integrity and security of internet transactions. Traditional methods such as passwords, PINs or tokens are highly vulnerable and cannot withstand sophisticated intruder attacks.

Stolen passwords or PINs can compromise the sensitive financial data of customers and lead to financial losses. Integrating biometric fingerprint recognition will help users to take advantage of the flexibility of internet banking while at the same time providing a high degree of reliability. Biometrics such as fingerprints or facial features is unique to each individual and cannot be spoofed by fraudsters. Most devices are now embedded with fingerprint scanner or webcam thus making it easy for the adoption of biometrics in online banking services.
INTEGRATING FINGERPRINT RECOGNITION IN BANKING AND FINANCIAL SERVICES SOFTWARE

Banking and financial services looking to enhance customer experience and security of financial transactions can utilize a complete biometric solution known as Touch N Go for integrating fingerprint recognition into their banking software. Touch N Go is a developer friendly biometric solution that allows fingerprint recognition to be integrated easily and quickly into existing banking and financial services systems even with no prior experience and no learning curve. Due to the unique nature of the integration methodology of Touch N Go, fingerprint feature integration into existing systems does not take months or hours but can be completed with just four lines of code.

Touch N Go has various inbuilt features such as fingerprint deduplication and fingerprint quality checks. These checks are performed in the background and eliminate the enrollment of duplicate fingerprints as well as ensure the enrollment of only the best quality fingerprints. Touch N Go provides various features such as a high level of accuracy, security and a solid infrastructure that are crucial for the efficient operation of a banking system.

Touch N Go is flexible and has support for a variety of programming languages with inbuilt source code and applications for developers use. It is also a cost-effective and high performing solution with support for a variety of fingerprint readers.

CONCLUSION

Biometric technology is proving to be the best security measure against intruder attacks and cybercrime. The adoption of biometric technology in the banking sector will help to improve the security and convenience for customers as well as save the banks and financial institutions from vast losses due to the increasing cases of fraudulent transactions.
ABOUT AUTHOR

DANNY THAKKAR  
CEO & Co-Founder

Danny Thakkar is the CEO and Co-Founder of Bayometric, one of the leading biometric solution providers in the world. He has been in the Biometric Industry for 10+ years and has extensive experience across public and private sector verticals. Currently, he is chief evangelist for Touch N Go.
COPYRIGHT
Copyright © 2016 Bayometric LLC. All rights reserved. This white paper was written, designed, and created by Bayometric. Information contained in this whitepaper is the copyright of Bayometric. This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published, and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this section are included on all such copies and derivative works. However, this document itself may not be modified in any way, including by removing the copyright notice or references to Bayometric LLC, without the permission of the copyright owners. This document and the information contained herein is provided on an "AS IS" basis and Bayometric LLC disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any ownership rights or any implied warranties of merchantability or fitness for a particular purpose.

REFERENCES
1. Biometrics for Finance Applications - Tractica
2. Financial Biometrics Month: Four Unique Modalities - Find Biometrics
4. More Banks Turn to Biometrics to Keep an Eye on Security - NerdWallet, Inc.
5. Mastercard Rolls Out Biometric App - Planet Biometrics