**Biometrics in the banking industry**

Biometric technology, such as fingerprint sensors and voice recognition, has become widely popular in recent years with the boom in mobile applications. Organizations are now trying to make use of this technology and implement it to a wide range of areas. Particularly for banking industry, biometrics can play a vital role in fraud prevention.

With the prevalence of phone and digital banking, banks require innovative ways to authenticate their customer’s identity. Moreover, though customers want their information to remain secured, they don’t like themselves to be scrutinized through an excessive authentication process for a simple transaction. Yet, it’s imperative for banks to verify their customers before they are given permission to access an account over a website, phone, or mobile application.

Conventional password and PIN codes have proven to not always be successful towards achieving security. Not only do customers forget them frequently, but the hackers also gather their personal information through various techniques such as phishing or social engineering. Thus, banks and account holders face losses worth millions every year as a result of identity theft.

When we talk about biometric banking, it simply brings together security and convenience. Biometric technology depends on a single action instead of other multi-factor authentication methods. For instance, in phone banking, a customer can be simply authenticated on the basis of their voice recognition instead of a sequence of security questions and password retrievals.

Unlike paper documents that can be forged, or passwords that can be cracked, an individual’s characteristics are unique. With voice verification software becoming more sophisticated, an industry like banking that prioritizes security can considerably benefit. Tools nowadays not only identify spoken words, but also the tone and pitch of voice.

For cash transactions, biometric technology replaces the need to enter traditional PIN code with identity verification such as facial recognition, finger prints or iris scanning. This removes the concern of someone stealing your debit card and using it to take out your money from your account. With biometrics enabled [card procedure](http://www.cardzgroup.com/BankCards.html), customers will be required to verify their identity before they can cash out the money.

# Benefits of Biometrics in Banking

To ascertain highest level of security, banks are now transitioning towards biometric technology. It offers numerous advantages to the financial institutions as well as consumers such as:

* no multi-factor authentication needed
* no PINs and passwords needed
* low operational costs
* inability of hackers to exploit information attained through a data breach

The last point is of utmost significance. This means that even if cyber criminals succeed in getting your credentials, they cannot use the information to their advantage. Customers also don’t have to recall multiple passwords and can authenticate themselves with only one biometric authenticator.

# Types of Biometrics in Banking

Biometric technology uses measurable and distinctive human traits to identify an individual uniquely. Here, we will have a look at some of the common biometric identifiers in the banking sector.

## Fingerprints

This method is one of the widely used authentication methods in branch banking and mobile banking. Though its usage has declined in the past year as a result of pandemic-related consequences, it is still effective in mobile apps for authentication purposes.

## Palm or Finger Veins

This identifies unique pattern of veins in an individual’s palm or fingers. Since it requires bigger equipment, its use is restricted to ATM or branch banking instead of mobile use.

## Voice Recognition

Voice recognition is a key biometric in phone banking. It recognizes the unique audio characteristics of an individual. Integrated with artificial intelligence, voice recognition improves with capturing voice prints through regular conversations. It does not require any special equipment, passwords, or location.

## Face Recognition

It deploys 3D sensors and computer algorithms to identify a face by measuring the shape, position, nose, size of eyes, jaw, cheeks, and more. Face recognition is gaining popularity but the technology behind it varies according to vendors. For instance, iPhone X uses Apple’s Face ID for logging into certain mobile apps. Face biometrics can sometimes not work in certain situations such as light intensity, glasses, or facial surgery, etc.

## Iris Scan

Retina scan is a live detection technology and scans complex line patterns and colors in the iris. The technology can be installed at ATMs and mobile phones.

## Behavioral Biometrics

This is a relatively new area which requires machine learning and big data for analyzing a mix of behavioral patterns of an individual to create unique profile for them. These patterns include anything from how a person uses their mouse to how the keystrokes are made on the keypad. The profile also includes location and IP addresses.

# Handling Biometrics Data: Avoiding Potential Limitations

Biometrics data is personal to every individual’s identity. When we talk about security, there is absolutely no room for error in keeping the data secure, or protecting it from getting compromised. Passwords and PIN can be changed, but your personal characteristics cannot.

Another important aspect to consider is false-negatives. If a system fails to recognize an actual biometric which the customer has no power to change, it will result in a mistrust in the technology and lead to disgruntled customers. Hence, once a bank’s system completely relies on biometrics, it must be sophisticated enough to correctly recognize an identifier every time.

Similarly, false-positives are also a possibility. This can be avoided by including “liveness” factor. Its better if the system sees your face through a live camera or authenticates your voice with different sentences instead of scripted lines.

# Conclusion

Biometrics is an innovative technology that is rapidly changing the way we manage banking. Over the next few years, it will be interesting to find out how it develops and adapts to the expectations of customers so that it is easily accepted and implemented by both banks and its users.