Biometric Cards: A Contactless Technology with High Security

As the payments industry shifts from plastic to digital, the need is more and more increasing to provide customers with the latest payment technology.

Since the start of COVID-19, we have witnessed a decrease in the use of physical cards, and an increase in the use of virtual cards, which will continue to dominate in the future.

A rise in digitization and related online services is now a major change in the industry, and something that will continue to grow in the future as businesses focus on digital transformation to adapt and innovate during these new tough and challenging times.

In order to adapt to this new situation, businesses will need to MAKE MOST PAYMENTS TOUCHLESS; the fear of contact with contaminated surfaces has given a real boost to the use of contactless payments, cards and wallets based.

One of the major innovations that the payment industry is implementing on the road to empowering a cashless world and to provide clients with the latest payment technology is the "*BIOMETRIC CARD*", a combination of contactless technology, advanced privacy and security, along with a simple fingerprint!

Why biometric cards?

The advantage of biometrics over other security procedures is that it is part of an individual and directly corresponds to his / her identity. Biometrics meet the requirements of authentication, non-rejection, confidentiality, and integrity.

Traditional passwords are proving to be less secure, and the next level to authenticate a person / card is the use of biometrics to verify a person's identity. Biometrics can be applied as a way to identify a person, and their utilization can help protect people from being a victim of identity theft. HOW?

1- The cardholder becomes the password

Fingerprint recognition is a very reliable and accurate way of authentication, and is very popular because of its familiarity and usability.

Fingerprints are unique to individuals and are therefore more reliable in verifying identities than a password, or asking various security check questions.

In the cybersecurity industry, biometrics are now considered as one of the best ways of protection when it comes to securing identities.

2- Protecting Business Data

The rapid growth of the internet and the high usage of e-commerce applications have pushed organizations to look for stricter security controls, and to start considering identity based security (biometrics) as important as physical security, since business and financial data must be protected from unauthorized access.

Biometrics are specific to individuals, which makes it very difficult to break biometric security protocols.

3- Optimizing Security with Biometrics

The advantage of biometrics over other security systems is that they are part of an individual and correspond directly to the individual's identity.

The application of fingerprint based biometric tools can notably increase the security of data stored on a card, or on an electronic device such as a personal computer or a company computer. Therefore, organizations and individuals aiming to strengthen the security of their networks, systems, and data can easily achieve this target by implementing biometrics.

Biometric cards and biometric authentication present several advantages from a Fraud, Security, and Money Laundering perspectives:

1- High Security and Guarantee:

Biometric Identification helps authenticate the identity. Most user's passwords, PINs, and personal identifying information have likely been compromised with a data breach, and therefore scammers who preserve the answers to traditional verification methods can have access to billions of accounts.

Implementing biometric authentication helps blocking the way on fraudsters and allows only a real, authorized user to access the account / card. In addition, biometrics can only be provided by living, breathing people, and a robot for example would have a hard time passing an iris scan.

2- Hard To Forge or Steal:

Biometrics such as iris scanning, face specimen, fingerprints, and others are almost impossible to duplicate with the current technology. There is almost no chance that someone's fingerprint or face specimen will match up exactly with someone else's. Therefore, it is very hard to find a cardholder having the same fingerprint as a hacker trying to breach a card secured by biometrics.

3- Convenient and Fast:

From a cardholder's point of view, it is extremely easy and quick to use biometrics. Placing a finger on a card is faster than typing out a PIN. In addition, forgetting a PIN is a common mistake of many cardholders. The chances of someone forgetting his own biometrics are impossible.

4- Non-Transferrable:

Everyone has access to a Unique Set of Biometrics.

A cardholder cannot transfer or share a physical biometric digitally, and the only way to apply biometric authentication systems is with a physical application.

In conclusion, approaches towards digital ID and the perception of digital identity are fundamentally changing. Since security in banking is becoming crucial, financial institutions have to set much higher standards when it comes to secure ways of confirming a client's identity for authorized transactions. And there is no better way to do it than implementing BIOMETRICS.

By: Nadine Ghosn

Founder and CEO – BeyondComply