Can biometrics provide a way for secure and easy online payments?

According to the South African Fraud Prevention Service, identity theft has increased by more than 200% in the last six years and is costing the country at least R1 billion per year. This growing cyber risk has brought with it t need for watertight methods to protecting personal data.

©Sergey Nivens via 123RF

Demanding and tech-savvy users continue to exert extreme pressure on companies to solve the convenience versus secu conundrum. This is where a seamless customer experience and data security intersects. In today's mobile world, it is increasingly important to have secure, on-the-go authentication. As a result, many experts feel that biometrics offers the b hope.

A new research report by analyst group BIS, forecasts the global biometric market to grow from $10.08 billion in 2014 to $25.31 billion in 2020. This steep growth projection is helping to fuel innovation that is evident in how biometrics modalities continue to spread across the human body. It started with fingerprints in the late 1960s and progressed to facial recognitic Today the list includes vein, palm, iris, voice, gait, DNA, handwritten signatures and tattoos.

The new wave of biometrics technology is gesture related and personalised through a combination of wearable technology and geolocation as well as sci-fi inspired implants and ingestible tokens. Facial emotion recognition technology is patent-pending and is pipelined for consumer use. Though these have appeared in films for many years, they are largely unprov in the real world.

A bad rap

Despite its association to the tourism industry's recent reduction in visitor numbers, biometrics in South Africa is enjoying real world resurgence.

Speaking at the Biometrics in Financial Services conference, Nick Perkins, divisional director for identity management at Bytes Systems Integration believes the reason is that we have arrived at a time where we need a new solution. "The existir card and pin authentication model has not been replaced because it is simple. The problem is that it's no longer secure ar is being exploited," says Perkins.

Essentially biometrics is the measurement of a human being through their physical characteristics. Physical biometrics is turned into electronic biometrics when an algorithm converts an image of a biometric subject into a mathematical string tha

can be best described as coordinates and descriptions of unique identifiable features. These algorithms then compare a "fresh capture" to the "reference template" which is warehoused in a database. The storage of templates instead of image helps to secure biometric data.

The many biometrics modalities on offer may hold the key to its wider adoption. South African biometrics experts agree th today it is not good enough for banks and other companies to rely on one form of authentication. PayU COO, Johan Dekk believes a solution lies in multi-factor authentication. "The dual-factor authentication model strives to have two of three verifications in place at all times. A pin code is what you know, a smart card is what you have and a biometric characteris is what you are. A one size fits all approach would not provide enough adaptability, security and redundancy in the event an access breach," says Dekker.

Much work to be done still

Authentication is not the only aspect of biometrics that requires smoothing out. Biometric data can be stolen, lost or otherwise compromised while being stored. Unauthorised access to biometric storage devices through corporate sabotage by disgruntled employees is a growing threat to privacy. So too, is the misuse of a biometric, given that the biometric itself cannot be changed. Once compromised it will continue to be an issue for the life of the donor, as opposed to a password which can be easily changed.

Independent identity verification expert, Dawid Jacobs, highlights a key focus area and a potential driver of biometrics tod Says Jacobs, "The emphasis is on customer experience and how quickly they can be helped. This creates an allowance f potential problems which escalate over time, especially with acceptable losses. In my view, there is no such thing as acceptable losses due to identity theft. The individual needs to be put back in control of their Identity."

The rush to ensure users are happy and safe

MasterCard is currently piloting its new biometrics app, MasterCard Identity Check, which is set for a widespread launch i 2016. The app combines facial or fingerprint recognition as well as the recent human obsession, selfies. It remains to be seen whether Mastercard have solved the problems associated with lighting and background. All fingerprint scans remain your device and facial scans are linked to the cloud so that templates will transmit and remain safe on MasterCard's server

Apple has applied to use a facial recognition system for photo distribution. This calls into question the company's pro-priva stance should it decide to use cloud-based processing or storage of private user info. Apple was also recently granted a U patent that covers a new technology that enables users to unlock future iPhones by...wait for it...taking a selfie.

Closer to home, Standard Bank has debuted its biometric banking app. Capitec has fingerprint details of all 6.2 million of i customers and has linked its biometric database to the Department of Home Affairs' database, enabling it to verify custom identity. The rollout of Biometric ATMs by FNB is imminent.

Dawid Jacobs is building an independent database of certified living and deceased fingerprint identities. He aims to provic SA companies with full audit trails and to be fully compliant with POPI, ISO and all relevant legislation. Jacobs says, "The more companies know about their customers and the more they collaborate the less pressure is on state law enforcement agencies who do not have the tech or the capacity." This will complement the FICA endorsed Know Your Customer initiati which also endeavours to prevent identity theft and money laundering.

Mustapha Zaouini, PayU's MEA CEO sums up the reality for all users. "The issue of protecting individual data will only gro in importance. In order to reap the convenience benefits, users must prepare themselves for more disciplined and multiple information security practices in this brave new world."

For more, visit: https://www.bizcommunity.com