




# Insight

New biometric approach for a  
challenging world



# New biometric approach for a challenging world

## At a glance

- 4 minute read. 
- The number of cyber-attacks and security events is growing exponentially .
- Multi-biometry authentication is user-friendly and very natural, and second, it keeps cybercrime away.
- How does it work?



The number of cyber-attacks and security events is growing exponentially and CSOs are struggling to protect their companies' data and transactions.

Most intrusions into corporate systems are aimed at hacking personal data, identity information, credit card numbers or IBAN in order to then proceed with fake transactions.

Those intrusions are made possible through authentication passwords which are easy to counterfeit, or to guess if the password is basic for 50% of known cases.

Security breaches through passwords are increasing and directly affect corporate operations (deny of service for the banks) or impact internal money transfers or external end-user payments (mobile payments). An impressive figure of 5 Billion card details were stolen worldwide (2016 Nilson Report).

Security leaders are facing increased

costs, losses and their company reputation; they are looking for new methods to better protect their investments and core business.

Fortunately, there are ways to block hackers by replacing the classic password

“WFnap&2Z\*\*”: for instance, multi-biometry authentication.

**“First, multi-biometry authentication is user-friendly and very natural, and second, it keeps cybercrime away from your operations when the password fails.”**

First, multi-biometry authentication is user-friendly and very natural, and second, it keeps cybercrime away from your operations when the password fails.

Currently, and more specifically, in the golden age of piracy you have with multi-biometry authentication a navy that can protect your boat. For example, a corporation can implement a biometric single sign-on for their users to protect the VPN access; a Bank can implement a biometric solution for corporate or private portal access on the internet. Furthermore, transactions where your ID can be counterfeited and compromised are now highly protected by multiple biometrics.

## How does it work?

During the connection to a secured space, thanks to multi-factor biometric authenticators, the user is invited to authenticate with his physical characteristics pertaining to every individual such as fingerprint, voice, face, iris and behavioural signature or keyboard dynamics.

To raise the level of security a double-step biometric authentication process is possible. It means that the authentication platform performs a double check: the first one compared with the data stored on the mobile terminal and the second compared with non-biometric desensitized data on a server. In this way the security is at a maximum and keeps away cyber-criminals.

Furthermore, the authentication platforms propose a full compliance with PSD2 and GDPR European regulations by performing a fully multi-factor anonymous authentication. All the data are de facto unusable in case of a hacking attempt because there is no personal data stored in the database; the storage format is prevented from restoring a clean copy of the biometry to identify a person as the data format itself is not reversible.

In conclusion, the top security challenge today and tomorrow for CSOs is to find a more effective way to secure access or transactions, and biometry is definitely one of the tools that proves greatly efficient in decreasing fraud and identity theft.

The benefits of a fully patented biometric authentication platform are

to significantly enhance security around corporate operations, gain greater control over who is able to access critical applications and critical data, and a bottom line bringing strong protection on corporate investments.

*Christopher Richard and Yves Chemla are Co-Founders of UNITED BIOMETRICS, who developed a strong multi-factor authentication platform for Banks, Enterprises, Carriers and Internet Players losing money from a huge fraud caused by large cyber-attacks and intrusions.*

*United Biometrics is compliant with the new European Directive PSD2 which requires at least 2 authentication factors and GDPR for protection of personal and private data. Major use cases are centred on cyber-attacks and terrorism intrusions: protection of IoT ecosystem, protection of payment platforms, protection of IT assets, protection of Data, protection of corporate user and private user on-line banking portals, protection of mobile payments, and protection of the Blockchain.*

*For more information:*

**United Biometrics Website**

[www.unitedbiometrics.com](http://www.unitedbiometrics.com)

