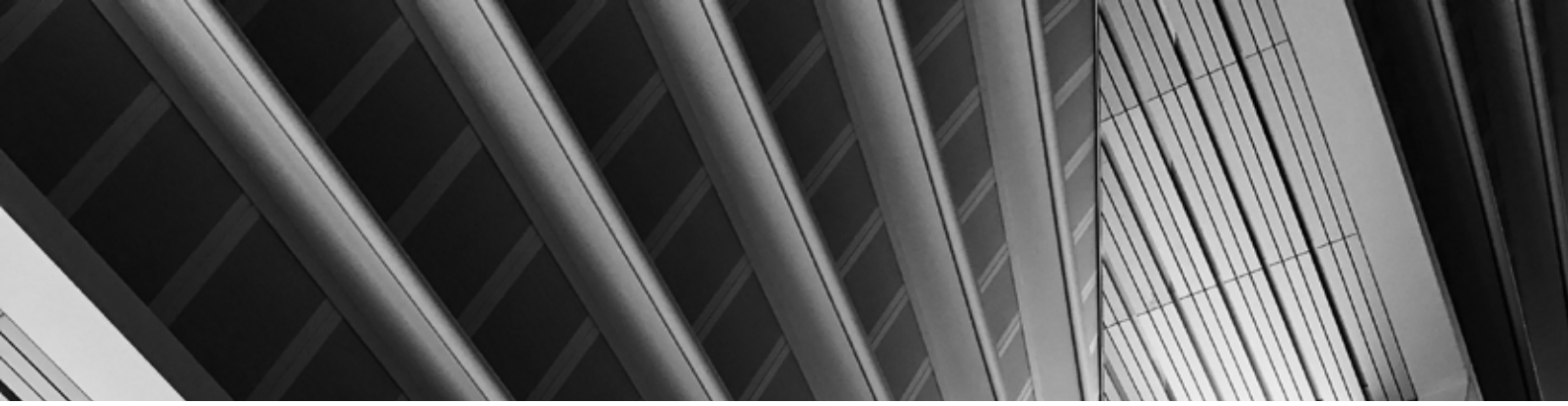
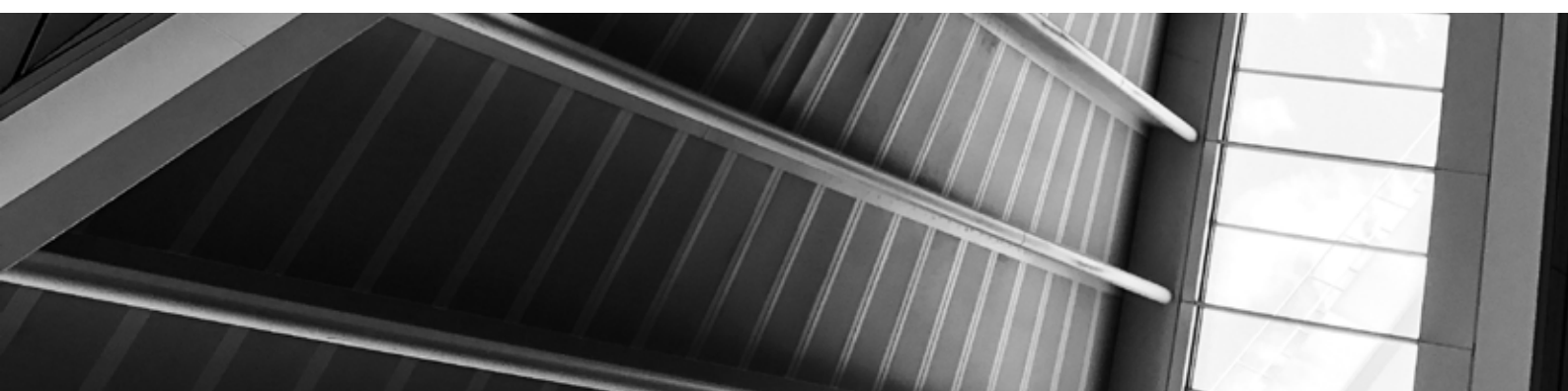


Insight

PSD2 and GDPR – Will Big Banks Be Ready for the September 2019 Deadline?



PSD2 and GDPR – Will Big Banks Be Ready for the September 2019 Deadline?

At a glance

- 4 minute read
- The European Commission Voted In an Important PSD2 Directive
- Fraud is Definitely a Growing Pain
- The Biometric Technology is Designed to Better Serve the Security Needs of Banking Customers

The European Commission voted in an important PSD2 Directive which sets out rules with strict security requirements for electronic payments and the protection of consumers' financial data, guaranteeing safe authentication and reducing the risk of fraud.

The clock counts now and Financial Institutions (FIs) must be ready for compliance with PSD2 for the September 2019 deadline.

> "The clock counts now and Financial Institutions (FIs) must be ready for compliance with PSD2 for the September 2019 deadline."

The PSD2 main requirements make mandatory a two-factor authentication (2FA) to be implemented for securing electronic payments within the 27 European countries.

Fraud is definitely a growing pain and a very serious concern for financial institutions, banks and insurances. Cyber-crime is increasing with more and more sophisticated schemes to corrupt data, to totally destroy areas of services, to make false transactions and payments, and even to modify supplier data. Security leaders are really struggling to keep-up with the severity and volume of those cyber-attacks.

As an example, the CEO sends you an email "Hi James I urgently need all details including account numbers of our supplier XYZ..."

If you are a responsive CFO, you will immediately send back all information to the trusted mail address of your CEO. Not surprisingly, in such a case the "supposed CEO" is a cyber-criminal who will modify the account number and immediately get all money transferred to the supplier credited to his own account within a couple of hours. Cyber-gangs use multiple tools, knowledgeable people and multiple locations, during a very short window of time for crime execution making it almost impossible to track them back, after the fraud.

According to McKinsey, CEO fraud has jumped 270 percent most recently and has led to losses of more than $2.3 billion over the last few years.

For big banks, fraud control and biometrics to replace passwords are seen as a real competitive differentiator and a way to attract new clients, both in corporate segments and retail banking. It is now a fact that biometric authentication for financial institutions and corporations are a serious alternative to passwords and comply with European PSD2 Directive by providing two strong authentication factors to the end-user.

Sensors are more and more reliable and available on Android and iOS marketed devices. Classic biometries and behavioural biometries can now be combined to offer a superior protection:

"Sensors are more and more reliable and available on Android and iOS marketed devices. Classic biometries and behavioural biometries can now be combined to offer a superior protection."

for instance a fingerprint combined with a signature (secret path), or a face combined with voice including anti-spoof capabilities. As an example, the face biometrics authenticates customers through their face, unique to each person. Bank clients can then enroll by recording their faces, which the bank will use to authenticate the person by matching live biometrics with the anonymous tag on the server. Each anonymous face will be uniquely tagged and cannot be reverse engineered once stored, because of the desensitized data.

Specifically, the enrolment provides immediate anonymization of the user profile; then hashed biometrics and data transformation issued from the hash, will offer a desensitized format data storage, therefore privacy and data protection are native standard to comply with GDPR Directive.

The biometric technology is designed to better serve the security needs of banking customers.

Remembering several passwords, plus several PIN codes, plus different challenges and questions, makes the process very complicated and does not solve the problem of fraud and cyber-criminality. With multiple biometries available on the smartphone, on the tablet, or on the PC, customers are now offered a very smart authentication, much faster, far more secure, and get a much better customer journey and experience at the end.

Security initiatives require strong use cases, such as protecting access to corporate portals or securing corporate payments, to get a quick pay-back and big savings in direct fraud charge-offs. By deploying biometric systems as a key element of their security ecosystem, financial institutions are cold-shouldering the hackers and cyber-criminals and will definitely win the game against fraud.

Cost and Return On Investment (ROI): Strong Biometrics Multi-Factors can quickly push the ROI down to zero. It is commonly admitted that the total cost of service to deploy and maintain the solution VS Fraud cost is in-between a couple of weeks and a couple of months of Fraud cost per year, depending on customer profile size and markets (Corporate/Retail).

Christopher RICHARD and Yves CHEMLA are Co-Founders of UNITED BIOMETRICS, which has 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. Use cases are centered 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 further information, visit:

unitedbiometrics.com

UNITED BIOMETRICS