Banks and the
Digital Trust Challenge

www.galitt.com

About Galitt

As a reference in the domain of payment systems and electronic transactions, **Galitt** is the market leader in France in every one of its business sectors, and throughout the world for its testing tools and its expertise in innovative technology.

Galitt is recognized for offering a wide range of skills and complementary knowledge to assist its clients throughout the lifecycle of their projects and in every link of the payment value chain. The company's size allows it to take on large projects while retaining its ability to be reactive, its personal touch and the ambition of an organisation that is run on a human scale.

Galitt is the reference in the execution of the most advanced payment technologies and the definition of tomorrow's technological architecture.

Galitt's services are based around 5 Business Units:

- **Payment Consulting** experts and their innovative approaches inform and enlighten our clients' strategic decision-making;
- **Payment Services** consultants help our clients with the execution of their payment projects;
- **Testing Solutions** teams develop testing software and take part in both the industrialisation phase of testing and the certification of solutions;
- **Payment Solutions** associates develop and operate high added-value e-money and transactional applications;
- **Payment Education** trainers pass on Galitt's expertise and experience during our training seminars.

Galitt is a Sopra Steria Group company. In 2018, Galitt achieved a turnover of €34.4 million and employed 260 people.

To find out more about Galitt, please visit our website, at: www.galitt.com

Contact Galitt Payment Consulting:
Rémi Gitzinger
Executive Director
+33 6 20 66 77 40
r.gitzinger@galitt.com

About this white paper

This white paper is addressed to a banking and financial sectors audience. Relying on the skills of Galitt Payment Consulting team, the following research tasks have been carried out to extend our analysis:

- A regulatory study, by reviewing PSD2, NIS directive, the GDPR and eIDAS regulations;
- A continuous regulatory & technological watch of digital services development in the banking / financial domain, including Buzz-Paiement[1] newsletter;
- An in-depth research on the subject of digital trust, particularly through the completion of a quantitative survey of over 800 people, from a representative cross-section of the French population coming from an Internet panel[2];
- Number of interviews with digital, banking and data protection experts to explore the different existing opportunities in terms of new services or customer experiences.

This document is particularly intended to:

- Analyze what is at stake with digital innovation in the banking and financial sectors and provide an executive summary;
- Understand the European regulatory framework which oversees the digital services and data usage / protection;
- Outline the banks' position as legitimate, trusted parties;
- Identify the general public's needs and expectations in terms of banking and financial services, and;
- Work out the opportunities for added-value services.

The objective is to understand the challenge set by digital innovation within the European Union for the banking and financial domains, and to provide an insight into the related opportunities.

1 Weekly newsletter covering news and innovations in the field of payments, in 1,000 words, produced by Galitt.

2 Survey carried out in July 2018 via Panel To Luna, based on a sample of 858 people, representative of the French population.

Contents

Introduction

The digital era confers an unprecedented strategic value to personal data. Collecting, analysing and exploiting an increasing volume of data along with the ever-increasing use of the Internet and digital services have become key activities of the data brokers and social networks juicy market.

This market is also notable for its opacity: the users of these networks, despite knowing that their data is being sold, aren't really aware of the exact purpose and even less of the scale of this exploitation. The April 2018 Cambridge Analytica scandal involving the use of millions of users' data for political purposes[3], unveiled the risk of people finding their personal data being recovered and exploited without their knowledge.

This downward spiral underlines the importance of both user consent and data protection. Now the European Union notifies these practices as violation of fundamental rights. With GDPR (the General Data Protection Regulation)[4] entry into force since May 25th, 2018, heavy penalties may be pronounced. As a result, GAFA and any other company would not freely exploit the data of European user without user's free and explicit consent, otherwise facing the sentence.

GDPR is aimed at restoring user trust in the digital services which has been weakened by the multiple large security breaches observed recently[5]. In addition, the complexity of the technology increases this mistrust, leading some users to reject services.

Mass market adoption to digital services is therefore dependent on the trust placed in these services. For the banking sector, trust - given the nature of the services provided - is already a crucial factor which takes on an even more key role when considering the digital transformation being operated as part of the modernisation of the banks' internal processes and the renewal of their service offer. The banks' challenge is to maintain customers' confidence and seize the opportunities created by digital innovation to strengthen it.

3 *Investigations by The Guardian and The New York Times revealed that, during the last US Presidential campaign, the Cambridge Analytica company managed to collect profiles and other data from millions of American voters to be used to fine-tune the politic strategy within the Donald Trump campaign.*
Refer to The Guardian article: "Cambridge Analytica execs boast of role in getting Donald Trump elected".

4 *EUR-Lex: GDPR regulation.*

5 *See The New York Times article: "Facebook Security Breach Exposes Accounts of 50 Million Users." Although one of the latest major cases in the media refers to Facebook, other major companies have also been affected: Yahoo, MySpace, eBay, Orange and more.*

1

Trust, the key issue for banks

Banks have managed and protected their customers' funds for centuries, adapting, as time passes, to changes in technology, regulations and operational methods. The current challenge for the banking sector is to avoid the fall-out from the scepticism and mistrust of users concerning digital technologies.

The survey carried out by Galitt of more than 800 French people of between 18 and 75 has allowed assessing the public perception on the banking sector generally, and particularly their views regarding to trust and data protection.

The protection and preservation of personal data is set with an average score of 8.5/10.

Along with the French unveiling to be concerned about their personal data, the question of who should be in charge of its protection becomes crucial.

In answer to this question, 63% of French people - including all age brackets - prefer to entrust their personal data to their retail bank. This figure is twice as high as the proportion of respondents preferring the French government. In third position, the "Online Banks" are preferred by a much smaller number than the traditional retail banks, but still with a significant score, considering their market share in France. Finally, we should also point out that 15% of those surveyed didn't want to entrust their data to any of the parties on the list offered.

Some differences appear when separating the different age groups. The youngest seem more willing to entrust their personal data (*only 8% in the 18-24 range didn't want to leave their data with any of the parties listed*), and have less apprehension concerning new companies (*17% would give their data to neobanks, as opposed to just 5% overall*). For the oldest age groups, these trends are reversed.

Retail banks and the government are the two actors which have the most consistent rates of positive response throughout the different age groups.

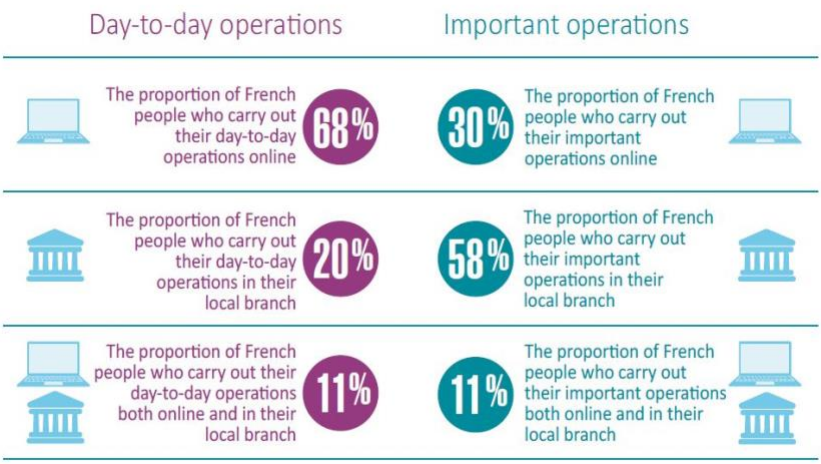
1.1. Trust maintained by a close day-to-day relationship …

Banks have succeeded in gaining the trust of their customers over the years by accompanying them in their day-to-day life. Indeed, people turn to banks at every major stage of life: taking out a student loan, getting a new car or buying a flat or a house[6].

Although 68% of those surveyed carry out their day-to-day operations online, 58% prefer to go into their branch for important banking operation, such as taking out a loan. This physical presence is clearly a key element of the day-to-day relation.

It is therefore important for retail banks to preserve it, especially given the finding that 60% of people trust a bank with a network of branches more than an online bank with no branches. 84% of those surveyed also believe that the presence of a personal banking advisor is either important or very important

6 *For more details on the life cycle of a bank customer, refer to the Galitt White Paper entitled "Le secteur bancaire face au mythe des Millennials : décryptage d'une génération aux multiples facettes" (French edition only).*


Day-to-day operations
Important operations
The proportion of French people who carry out their day-to-day operations online
68%
30%
The proportion of French people who carry out their important operations online
The proportion of French people who carry out their day-to-day operations in their local branch
20%
58%
The proportion of French people who carry out their important operations in their local branch
The proportion of French people who carry out their day-to-day operations both online and in their local branch
11%
11%
The proportion of French people who carry out their important operations both online and in their local branch


The proportion of French people who have more confidence in a bank having a branches network than in an online bank with no branch
60%
29%
The proportion of French people who have the same confidence whatever the bank has a branches network
4%
The proportion of French people who have more confidence in an online bank with no branch than in a bank which has a branches network


The importance of a personal banking advisor for French customers
0%
20%
40%
60%
80%
100%
Essential
38%
Important
48%
Useless
15%

1.2. … And legitimity won through technical expertise and banking know-how

Retail banks have true expertise in security matters and financial technology. They have infrastructures and technological tools enabling them to protect their customers' assets, including money and data. Just as with personal ID data, bank credentials are considered as confidential personal data, which, for the customers, justifies the need of protection.

PERSONAL DATA

As defined in the GDPR[7], personal data is "any information relating to an identified or identifiable natural person". Further clarification states that, "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."

Furthermore, customers put confidence in the payment means and related security provided by banks. In particular, the currently used OTP (*One-Time Password*) SMS authentication method as part of the 3D-Secure protocol was rolled out in 2007, and is well established as a security measure for e-commerce payment transactions[8]. Indeed, 68% of those surveyed feel that the security measures implemented by the banks reduce the risk of fraud, and 72% believe that the measures in place for online identification, either to make a payment or to gain access to personal home banking account, are secure - including 16% who said "very secure". The professional know- how, including KYC (*or "Know Your Customer"*) procedures, helps make the customer relationship more secure and give greater legitimacy to the bank as a trusted party.

7 *See part 2.2 for more details.*

8 *According to the Banque de France annual report of the French "Observatoire des Moyens de Paiement", published on 10th July 2018, 41% of the total online payment amount is authenticated by 3D-Secure.*

KYC

European Directive AMLD4[9] transposition into French law sets out expectations of KYC processes for customers and beneficiaries identification and identity check. KYC is an identity checking procedure, which consists in collecting, analysing and verifying personal data, as well as evaluating risks. In the case of a transaction, banks now must complete this analysis process via KYC not only for their customer, but also for the beneficiary of the transaction. Some banks have started offering remote identification solutions relying on biometrics technologies enabling enhanced KYC procedure, and thereby reduce the risk of fraud through stolen identities. The goal is to keep the same level of security as a face-to-face KYC process.

By linking the customer contractual agreement in such a process, the bank ensures the reliability of the provided identity. For every online transaction, the customer will have to authenticate theirself, thereby proving to the bank that they are who they claim they are. From the customer's point of view, this authentication procedure based on a verified identity is seen as more secure: Indeed, they know that no one else can access to their bank account.

According to the survey carried out by Galitt, 69% of French people do not find this process a reason to drop out the application for opening a new bank account, even though many details are needed. On the other hand, 53% of those surveyed have already dropped out an online shopping cart because the company involved was asking for too many personal details.

9 *See part 2.2 for more information related to AMLD4.*

The French, when it comes to an enrolment process which requires a lot of personal data, attach greater importance to, and have more trust in, banks than other web companies in general. This public mistrust of a number of services, and particularly of social networks and of Telecom operators is partly due to the various scandals involving leaks and resale of data. Banks, thanks to the close relationship they have with their customers, as well as their professional know-how and the technology they use, can style themselves as a trusted partner and this gives them an excellent competitive advantage on the question of data protection. The banks therefore have the advantage to be able to offer supplementary services in this sector.

1.3. A relationship of trust which can be strengthened

Even though the banks are well regarded as far as their ability to protect their customers' personal data is concerned, the level of confidence that French people have in them could still be strengthened, as the overall trust score given to them is 6.6/10.

This trust is limited by two main factors: fees which are not always seen as fair and a lack of transparency, particularly when it comes to their fees policies and the use of personal data (*for profiling and scoring*).

As an example, a customer won't always understand why their application for a loan has been refused, following profiling and scoring[10]. A change to incorporate more transparency, within the framework of GDPR, would help improve confidence (*e.g. a request for free and informed consent from the customer about the institution's practices*). Thus, banks could use profiling and scoring as non-discriminatory, or even positive, tools (*e.g. in the fight against over-indebtedness*) which benefit both bank and customer

PROFILING

In the words of the General Data Protection Regulation (*GDPR*), profiling means "any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements".

We should note that security is the third approach identified as likely to improve trust amongst French people. This shows that, despite recognising the banks' expertise in data protection, the public wants security to remain a priority as banking activities are transferred into the digital realm.

These areas for improvement need to be analysed in the light of current market developments, characterised as they are by the appearance of new challenges, new regulations, new players and new technology.

10 *Scoring: giving customers a score based on the risk analysis result that is produced when profiling.*

2

A changing market: redefining the nuts and bolts of trust

The banking market is currently being turned upside down by regulatory, competitive and technological changes. These factors, which are sometimes closely linked, are radically affecting the nuts and bolts of trust. In particular, data protection is the purpose of a Europe-wide dedicated regulation, the GDPR. This changing landscape gives a strategic dimension to digital identity.

2.1. Digital identity, the new issue at the heart of trust in the digital world

Digital identity is the representation of an individual in the virtual world. It consists of a set of attributes, linked to a natural or legal person, which exists on the Internet or within an IT system. Indeed, digital identity isn't limited to minimum ID data set[11], particular to the sovereign identity of a person, and can be defined as a specific digital representation of that person, which could be more or less anonymous according to circumstance. One person owns several digital profiles which make up his or her digital identity. Typically, a set of attributes collected on the Internet and directly or indirectly connected to a particular person (email address, pseudonyms, IP address etc.) would allow a digital profile to be created.

Digital identity is at the heart of enrolment and identity checking processes, authentication, signing and consent management, whose functions require an individual's personal data to be used.

The identification function aims to answer the question, "Who are you?". During the enrolment step, this function involves collecting direct (*name, email, personal ID data such as a social security number*) or indirect (home address, age, gender, etc.) Personal Identifiable Information (*PII*). This function also includes identity verification of the person (*checking validity, authenticity, totality and the unequivocal link to a specific, actual person*). The identification process enables the person whose identity is thus validated to legitimately access to the service.

The authentication function answers the question, "Are you really who you say you are?". It intends to grant access to services and/or rights associated to a specific person, by formally verifying certain information that is qualified as one or more authentication factors[12].

Some services (*e.g. access to a social network or to one's personal email*) do not require authentication based on an identity which has been checked beforehand

11 In France, this data set includes: first name, surname, gender, date of birth and country or town of birth.

12 These are classed in three categories: possession, knowledge and inherence.

via an identification phase. In this case, the person can use any choose any login data (*e.g. a pseudonym*) as information to grant access to the service.
For some other certain services (*for instance, the opening of a bank account*) authentication requires a verified identity, linked to a unique principal identifier, held in a database or register. In this case, online authentication aims to confirm the ownership of this identifier - and thereby the verified identity profile linked to it - by the user who is claiming it. A typical customer enrolment process for opening a new bank account includes a KYC process that requires customer iden- tification (including ID document check) and customer authentication (*checking that the request is truly issued from the person who has been identified*). When the account is being used, authentication determines access to a service a given identifier has a right to access to (*e.g. a payment means, by entering the payment card's PIN*). Since each service requires its own identifier and a means of authentication, users are facing the management of multiple passwords and the use of methods that have different levels of security. Meanwhile, PSD2 (*see the insert on PSD2 below for further information*), as set out in its own delegated regulation - RTS[13]- generalises the requirement for strong authentication for payment services. This strong authentication associates authentication with two different, independent factors with the creation of a unique, single-use code in order to avoid the risk of remote attacks and of the re-use of the authentication code[14].

13 *RTS: Regulatory Technical Standards: the complete set of technical standards prepared by the European Banking Authority in collaboration with the European Central Bank and the different national central banks. Various RTS are planned for by PSD2, in order to harmonise PSD2 operational introduction in member states.*

14 *See article 4-30 of PSD2 for a definition of strong authentication.*

PSD2

The PSD2 Directive[15] creates a framework for all payment services. The bill transposing this Directive into French law came into force on January 13th, 2018. To encourage the development of innovation, PSD2 enables access to, or sharing of, certain banking data via secure channels between payment service providers (PSPs). In order to do this, the Directive has been clarified by RTS setting out the open, common and secure standards for these communication channels. Therefore, the standard allows the definition of technical and organisational measures that control a new entitlement: that of allowing third parties access to payment data, which has to be explicitly agreed to by the user, as stated in the GDPR. The RTS describe, in addition to the setting up of secure interfaces, the procedures relating to Strong Customer Authentication (SCA), which is required when a customer accesses their payment account online, initiates an electronic payment transaction or carries out any action through a remote channel which may imply a risk of fraud. Strong authentication helps prove the explicit consent given by the user when he/she authorises access to their banking data for a third-party PSP. This consent also allows the latter to initiate a payment operation from an account held by the Account Servicing Payment Service Provider (ASPSP). The rules introduced by the RTS will all have to be applied as of September 14th, 2019.

Please note that these two functions - identification and authentication - can be directly guaranteed by the service provider that the customer wants to have access to, and which can thereby take on the role of the identity provider. However, the trend today is to pass this role on to a third party, with possible various software architectures: centralised (*the single sign-on model, e.g. Facebook Connect*), decentralised (the federated identity model, such as FranceConnect), and now distributed, thanks to Blockchain technology (*see part 3.1 for more details on this subject*).

15 *Galitt have also published a white paper, updated in 2018, devoted to the subject of PSD2 and how it affects the banking sector: "PSD2 & OPEN APIs: Threats and opportunities for the banking sector. Are we moving towards Open Banking?"*

THE "ACTION PUBLIQUE 2022" PROGRAMME

In France, the "Action Publique 2022" programme16 states that setting up secure digital identity solutions is a priority. It involves the roll-out of a secure digital identification experience for the state, and of the connected eIDAS methods of electronic identification. These will enable access to this experience and to the exchange of data between authorised identity provider and authorised service providers. The different actions will be carried out under the user's control, with a guarantee that their personal data will be protected. The programme also includes the principle of proportionality between the strength of the identification required (the personal data used) and the use. This service should be on-stream by September 2019. Other electronic identification methods, both hardware and software (for example, a mobile app) are currently following the qualification process as required by ANSSI (the French national cybersecurity agency) for integration into "France- Connect" by DINSIC17

The functions associated with digital identities are closely linked to the new GDPR rules, which tackle the subject of personal data for banks, on technical, regulatory and organisational levels as well as on the particular point of customer trust.

2.2. The General Data Protection Regulation (RGPD), illustrating the transformation of the regulatory framework

The **RGPD**, passed in 2016 and in force since May 25th, 2018 defines a framework of reinforced responsibilities to protect users' personal data. This regulation follows on from the 1995 directive[18] - never strictly enforced due to the weakness of and variance between penalties set by different member states - and indeed applies directly to every member state of the European Union without the need to be transposed into national law. Compared to the previous directive, GDPR reverses the relationship regarding compliance and introduces the idea of **accountability**. This means that every party responsible for processing[19] must be

16 *A programme launched on 13th October 2017 by the French Prime Minister which aims to speed up the public-sector transformation and works on reforms proposed by the 2022 Public Action Committee.*

17 *DINSIC : Direction Interministérielle du Numérique et du Système d'Information et de Communication de l'Etat (French Interministerial Board for the Digital Sector and State Communication and Information Systems).*

18 *This is Directive 95/46/CE (1995) relating to the protection of natural persons, concerning the processing of personal data and the free movement of this data (the key text before GDPR came into force).*

19 *Responsible for processing: French CNIL authority defines those responsible for processing as follows: "The person, public authority, department or organisation which determines the means and the ends of the processing of personal data, excepting in case of express designation by legislative or regulatory bodies concerning*

autonomous and able to correctly manage the protection of personal data and must guarantee continued compliance to GDPR rules. Audits can be carried out at any time, whereas the 1995 directive allowed for a fixed date to be set for controlling the measures in place.

GDPR sets out for the user a right to **transfer their digital data**. A customer must be able to recover their data and to transfer it smoothly and easily to another institution, should they wish to change. Failing that, they can turn to the supervisory authority (*in France, CNIL*) and to the judicial system either individually or as part of a group action.

GDPR strengthens the idea of **explicit, free and informed consent** concerning the collection and/or processing of personal data, even though it isn't required when fulfilling the obligations of a contract signed by the person concerned, nor when a legal obligation requires a measure of data processing. Despite all that, customers must always be informed of the collection and processing of their personal data as they are the sole owners of that data.

this processing. In practice and in general, this is the legal person which is embodied by its legal representative."

GDPR includes a variety of proposals for measures, particularly the principle of data minimisation. This measure involves reducing all requests for personal information to the strict minimum necessary to carry out the job in hand, and only for the time required by that job.

DATA MINIMISATION

Here is a concrete example: the registration path for a car insurance policy requires the user to provide personal data which should theoretically be limited to only what is strictly necessary (i.e. linked to the vehicle, its use and the customer's driving licence). This data can be held for a period not exceeding five or ten years, depending upon the nature of the policy, starting from the expiry of that policy. The insurance company may ask the customer to provide extra information (which is not required for the provision of the service), but their explicit and informed consent is needed to do so. An example could be the customer's marital status and number of children in order for the insurer to be able to carry out statistical studies and to provide extra services not included in the policy. However, asking the name and age of these other members of the family will not be considered as legitimate under the principle of data minimisation.

Another key principle of GDPR which is especially pertinent for banks is **privacy by design**. In other words, it is the respect of the user's privacy rights from the conception and design of the service, and rights through its life cycle. This means that every new product or service which requires users' personal data must, from the first moment and throughout its period of use, guarantee respect of privacy.

PRIVACY BY DESIGN AND PRIVACY BY DEFAULT

According to CNPD (*Luxembourg's National Commission for Data Protection*), "the concept of Privacy by Design aims to guarantee the integration of privacy protection into all new commercial and technological applications right from the drawing board. For each new application, product or service which requires personal data, those responsible for processing it should offer users the highest possible level of data protection. As an example, a Privacy by Design system allows, following a request, access to a value or piece of information of interest which is connected to personal data, without revealing the precise data (*e.g. confirming whether or not an individual is over 18 without revealing their exact age*). The concept of Privacy by Design is closely linked to that of Privacy by Default, according to which every company which processes personal data must establish the highest possible level of data protection, by default. In this case, it is the user who maintains control over the settings."

Elsewhere, the banks are affected by the impact of GDPR upon profiling and the related automated decision-taking. For instance: during a loan application, the automated decision which results from the profiling carried out by the bank must be clearly and freely consented by the customer, who must also be able to object to, should they wish it, and ask for a human intervention. Customers can also ask to have access to the "scoring" numbers, the calculating method and the logic of the automated decision.

AUTOMATED DECISIONS

An entirely automated decision is defined by CNIL, within the framework of GDPR, as "a decision taken regarding a person, using algorithms applied to that person's personal data, without any human being intervening in the process. This can happen in several areas of business (finance, tax, marketing, etc.) and may result in legal or other significant consequences for the involved persons. For example, the decision to refuse a loan could be a result based purely on the use of an algorithm which has automatically applied some specific criteria to the applicant's financial situation, without any human intervention whatsoever."

Even when considering the risk of fraud, a 100%-automated decision can be prohibited. On July 13th, 2017 CNIL[20] stated that no decision resulting in legal consequences for the person concerned, and whose data was processed within the

20 *"Decision n° 2017-217 of 13th July 2017 on sole authorisation for processing personal data within the remit of the fight against fraud in the b anking and financial sector (AU-054), published in the official journal, 25th July 2017 (text n° 63).*

remit of the fight against fraud, could be taken solely based on automated processing. Since then, automatically-generated alerts shall lead to non-automated analysis by authorised personnel, in order to avoid impairing customer trust in the banks. However, there are still some, strictly controlled, automated decisions which are permitted by the authorities in charge of applying the GDPR rules[21].

Within the GDPR framework, other important definitions are recalled. One example is that of sensitive data. In France we should add the particular instance of the social security number, known as NIR, which holds a special status amongst sensitive data: a specific decree is required to permit collection, processing and storage of the NIR. For example, when collecting and storing a payroll on paper or digital form whatever, outside of the field of the decree, the NIR must not, or no longer, appear on it.

SENSITIVE DATA

In the words of CNIL, sensitive data is "all data referring to racial or ethnic origin, political, philosophical or religious views, trade union membership, and health and sexual orientation. In principle, sensitive data cannot be recovered and used without the explicit consent of the involved person".

Companies which deliberately infringe the GDPR **may face a maximum fine equivalent to 4% of their global turnover, or E20 million** (*whichever is higher*). Many digital projects can meet, de facto, some of the criteria imposed by the GDPR (*checks, proportionality*[22]). Banks must see these new regulations as an opportunity and not as a constraint.

According to CNIL, businesses can indeed take advantage of the application of GDPR in order to strengthen user trust, improve their commercial efficiency, better manage the business, improve their data security, reassure their customers and their payers, and, last but not least, create new services.

THE MARKET OF TRUST

In the "Nowadays, there has been a culture change, and people are looking to

21 For example, in France, the CNIL imposed some constraints on Boursorama Bank which had to keep to when it was allowed to set up an automated decision-taking system as part of its remote KYC processes.

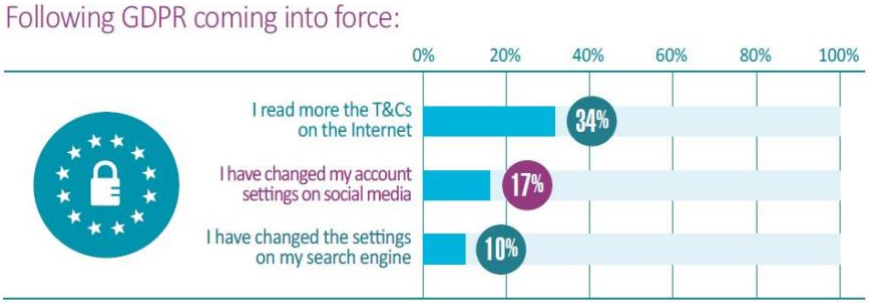
22 This is the principle whereby data held should be only that which is pertinent to, and strictly necessary for, the goal of the file it makes up.

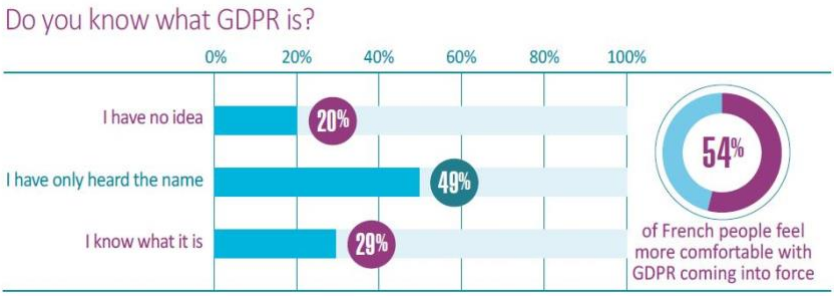
protect their data. Europe is sending a big message to the rest of the world in terms of respecting individuals. GDPR is a single law for all the countries of the European Union which enables to harmonise regulations. It is an opportunity for companies to position themselves as credible and trust-worthy forces, as well as a way to level the playing field between European and foreign companies and between multiple players. GDPR brings choice back to individuals. It is at the beginning of a new market: the market of trust. Investment funds, for example, have already decided to make GDPR compliance a decisive factor in their choice of investments."

Isabelle Falque-Pierrotin
Former Director of CNIL
at the Viva Technology Conference, May 25th, 2018 (*the day GDPR came into force*)

GDPR protects users from any abuses of their personal data. GDPR establishes a uniform regulatory framework for all member countries and brings more coherence to the application of protection measures, as well as penalties, concerning digital services which require the use of personal data.

The coming into effect of GDPR has been welcomed by users, even though many are still unaware of it (see infographic, below). A majority of French people surveyed said they were reassured by GDPR, more than a third take more time to read the terms and conditions on the Internet since the regulation came into force, while 17% have changed the privacy settings of their social media and 10% the settings of their search engine.




Do you know what GDPR is?
0%
20%
40%
60%
80%
100%
I have no idea
20%
I have only heard the name
49%
I know what it is
29%
54%
of French people feel more comfortable with GDPR coming into force

APPLYING GDPR IN FRANCE

In France, CNIL is responsible for enforcing the GDPR. From now on, it will be even more vigilant about the respect for the fundamental principles of data protection, even if they remain essentially the same as far as the French law on digital information and liberty is concerned: fair processing, relevance of data, retention periods, data security, etc. Companies will therefore continue to be subject to rigorous checks by CNIL and to possible penalties, as authorised in law since October 7th, 2016. Indeed, several companies have been punished for **security deficiencies on their websites, relating to the accessibility of customers or beneficiaries' data**.

The GDPR is only the first step in the management of new digital practices. The future **ePrivacy** regulation[23] should come into force soon to supplement GDPR and to widen the free movement of data to electronic communication within the European Union, while still establishing rules that respect the European Charter of Human Rights. It will bring an equivalent level of protection between all natural and legal persons and ensure the confidential protection of electronic communications (both content and metadata), as well as ensuring integrity protection of assets of both natural and legal persons. The ePrivacy regulation will allow direct marketing communication within a framework that respects the rights of users.

To summarise, banks have to be able to integrate the constraints of this battery of incoming regulations into their internal procedures. On the other hand, they will benefit from the opportunity to offer new, secure services based on the free movement of data and Europe-wide interoperability.

23 *EUR-Lex: a proposed regulation concerning respect for privacy and protection of personal data held within electronic communications.*

Focus on the banking regulatory framework

Banks must follow numerous regulations in order to protect their customers from risks that they might be exposed to. Banking regulations are governed by the international standards of the Basel Committee. The Monetary and Financial Code (*in French, "CMF"*), which integrates European regulations and directives into French law, draws up the regulatory framework which applies to French banks. France's national Prudential Supervision and Resolution Authority, ACPR, which answers to the French central bank (*"Banque de France"*), is in charge of monitoring banking institutions on French soil. The banks' activities are also supervised by specific rules and directives.

The European Anti Money Laundering Directive 4 (*AMLD4*), which came into force in January 2018, instructs banks, and all financial, payment and insurance service providers, in the fight against money laundering and financing terrorism. Its updated version - AMLD5 - will expand its range of operation to include cryptocurrencies, toughen up requirements in the field of prepaid cards and ease access to the European Transparency Register[24]. This directive should be implemented by January 10th, 2020.

The European NIS directive (*for Network and Information Security*), which came into force in May 2018, determines notions of OES (*Operators of Essential Services*) and of digital trust services. It was transposed into French law in 2018, to set out general expectations for the security of networks and information systems. ANSSI (*the French national cybersecurity agency*) defines the applicable rules and directs acts of regulatory compliance. The practices stated in NIS are, for the most part, already in place in France. Indeed, they continue the path forged by the French military planning law (LPM), which characterises major banking institutions as "Operators of Vital Importance" (*"OIV" in French law*), thereby making them subject to strict obligations in terms of cybersecurity. These obligations aim to insure the protection of the vital infrastructures they operate: a cyber-attack on the information system of an OIV could endanger the whole economy of the nation. The NIS directive could lead

ANSSI to categorising all payment service providers as OES, which would oblige

24 *European Transparency Register: according to the European Commission, this is a database listing all organisations which are looking to influence the legislative process and policy implementation of European institutions.*

them to apply certain rules on governance, protection, defence, resilience, reporting of any incident concerning security and auditing (*an annual information system check*).

Banks are also required to follow eIDAS regulation, which the first part purpose is the creation of a common European basis for interoperability and mutual cross-border recognition of digital identity for online access to public services. eIDAS specifies three levels of assurance[25] : weak, substantial and high[26].

The decree which modifies the CMF code and which aims to strengthen French measures in the fight against money laundering and financing of terrorism, recommends that KYC processes for customers and beneficiaries should be given electronic identification means that are categorised as 'high' on the eIDAS scale, or 'substantial' if they are supplemented by further measures. On this point, the decree pre-empts and complements the upcoming AMLD5 directive which mentions the possibility of making eIDAS-recognised electronic identification means available, but without specifying the level of assurance to apply.

The second part of eIDAS regulates interoperability and the legal standing of the five digital trust services[27] for the use of both public and private services. Many banks have already set up electronic signature facilities in order to simplify processes when it comes to dematerialisation. They can also take advantage of solutions put forward by eIDAS qualified service providers, so as to ensure the highest legal validity. According to the eIDAS text: "the legal effect of a certified electronic signature is equivalent to that of a handwritten signature". In other words, only a certified electronic signature is interoperable across Europe and be binding without the person needing to show proof in a legal framework (*with the burden of proof reverting to the opposing party*).

25 *According to the Appendix of Commission implementing regulation (UE) 2015/1502, dated Sept. 8th, 2015.*

26 *eIDAS specifies the requirements for each process (enrolment, electronic identification, authentication, and management and organisation).*

27 *Electronic signature, electronic seal, time stamp, electronic delivery service and website authentication.*

3

Digital opportunities: revamping internal processes and launching new services to enhance security and trust

Banks, when it comes to both internal processes and services offered, can take full advantage of the opportunities coming from the changes in the banking

market by relying on digital innovations.

3.1. New solutions for running banking businesses, strengthening security and data protection

New solutions, relying on technologies that are experienced to a greater or lesser extent, aim to ease, speed up and secure data management and processing by the banks. From customer enrolment to secure sharing with third-parties, and including handling personal data, there are so many possibilities which enable companies to become compliance with the new European legislation. Meanwhile, with access to personal data being increasingly facilitated with digitization, banks have the opportunity to set up *(in addition to the necessary technical and organisational measures*) specially-designed measures to protect their customers' personal data and to respect users' rights. In this way, banks would comply with the principle of Privacy by Default which is prescribed by the GDPR.

The blockchain, a technology for GDPR compliance?

Unveiled to the general public thanks to the Bitcoin phenomenon, the blockchain has since been the subject of many investigations and experiments, resulting in the launch of new services, particularly in the finance domain. One of the recurring themes, which is not specific to the financial sector, deals with the role blockchain could potentially play in the management and protection of personal data. However, questions can be raised about the match between the blockchain and the founding principles of GDPR, as the technology, by nature, does not allow applying the right to wipe or correct data. Nevertheless, compliance with GDPR is still foreseeable via an adaptation of the blockchain technology applied to a private consortium. According to CNIL, the idea of a private blockchain allows "a designated authority to keep control of transactions and potentially to check and rectify them".

In France, According to CNIL, "blockchain is a technology for storage and transmitting information, transparently, securely and operating without a central controlling body. It consists of a secure and distributed database which holds the history of all transactions carried out between users ever since its creation. It is shared between all its different users with no intermediaries; hence each one is able to verify the chain's validity. There are public blockchains, open to all, and private blockchains, for which both usage and access are restricted to selected actors. Therefore, a public blockchain can be assimilated into a large public, anonymous and forgery-proof ledger. Blockchain technology and Distributed Ledger Technology (*DLT*) in general, is usable in many different sectors, such as the environment, transport, logistics, education, health and finance[28] ».

As far as GDPR is concerned, blockchain provides the opportunity to offer a forgery- proof ledger thanks to the time-stamping of the blocks and the resilient integrity of transactions stored on blockchain. That opens up possibilities in terms of being able to track customer consent, transactions and any modifications to personal data, which lets businesses adhere to the principle of accountability with GDPR supervising authorities and to respect users' rights (access rights, modification rights) in a transparent manner.

However, if private blockchains restrict access to the information stored therein to the legitimate users, they don't solve the issue raised by the "right to be forgotten" (data removal), nor do they ensure data confidentiality, as each party with access rights to the blockchain is able to read all the blocks of that chain. This is why block- chain technology should be used for its primary function as a ledger; a distributed and secure registry of time-stamped transaction records, and not a distributed personal database.

Above and beyond its use as a book of record, blockchain technology can be combined with the use of "privacy by design" smart contracts that enable the automatic software fulfilment of transactions and clauses while abiding by the fundamentals of GDPR. The Ethereum protocol enables, since 2017, the use of a new cryptographic brick: the "zero knowledge proof", or **ZKP**[29], which aims to give confirmation of a piece of information without revealing the content. ING was inspired by this concept…

…to develop its own solutions. Its latest, Zero Knowledge Set Membership, lets a customer prove, via a KYC process, that they are, for example, a citizen of the

28 To see more about example applications, please refer to the European draft resolution on distributed registry technologies and blockchains to strengthen trust by disintermediation, published on September 24th, 2018.

29 This term refers to a secure protocol in which one party supplies a guarantee to a verifier that certain information relative to a secret is true, without revealing any more information about that secret (beyond the fact that it's true).

European Union without revealing their country of origin[30].

For some services such as financial services, this proof needs to have probative value, in the strict legal sense. In this case, blockchain technology - as a ledger evidence, whether connected or not to the functions of a smart contract - is not enough: the probative value of a piece of personal data (or "attribute") must be linked to a level of guarantee delivered and authorised by a trusted third party for a limited period of time.

Distributed ledger and blockchain technologies could really show their best side when it comes to managing these guarantee levels of probative value (writing, cancelling, prolonging and granting access). Thus, a service provider wanting to verify the reliability of a customer's personal attribute can rely on this type of ledger, supplied or managed by a trusted third party within an open and transparent trust ecosystem.

As a private, trusted third party, banks have a role to play in the establishment of these probative value ledgers and their functions. These ledgers can, in addition, act as a foundation for creating digital identity ecosystems. This is the direction that Canada appears to be going in, thanks to a large-scale initiative led by SecureKey, the specialist in authentication and identity validation. The company is bringing several major Canadian financial institutions on board and the project will bring opportunities to deliver new banking services to customers (see part 3.2 to discover these services).

Finally, blockchain is opening up new horizons on the subjects of managing personal data and KYC, which is also facing up to other innovations.

30 *For more information, please refer to ING's White Paper in Zero Knowledge Set Membership.*

Biometrics, a secure solution for remote KYC?

When it comes to KYC, the current movement is towards a completely digitised user experience. For banks, the time saved via an eKYC procedure when handling a customer file in undeniable: some banks can now open an account in 24 to 48 hours, compared to 10 working days for a standard procedure. As for customers, the enrolment process is smoother and one sticking point - the need to organise a physical appointment at a branch - is eliminated. On the other hand, other challenges have appeared: on top of the connectivity requirements imposed by eKYC, there are more security threats for the process, and particularly for identifying the prospective customer. The stakes are doubled, as banks must both remotely verify identity using some proofs of identity (e.g. a valid ID, a proof of address etc.) and be able to carry out a "liveliness detection" of the physical prospective customer.

In Europe, some economic or banking regulators - in particular, Italy, Austria, Spain and Estonia - have expressed a preference for this new style of biometric procedure, based mainly on enhanced videoconferencing solutions.

In France, ACPR has not made a public statement about identification systems via facial recognition of prospective customers when setting up a remote contact with them. However, CNIL, even before GDPR, authorised the remote validation processes set up by both Société Générale[31] and Boursorama[32], as following appropriate measures for protecting the particularly sensitive personal data that biometric data represents.

The two procedures are based on biometrics to allow a comparison between the ID photo and a selfie taken by the customer on his/her phone. In addition, Société Générale carries out its liveliness detection via a video interview between the prospective customer and an advisor. During this interview, another biometric comparison can be done between the original ID photo and pictures extracted from the video. If necessary, identity verification can be completed by the advisor using a questionnaire.

Boursorama, on the other hand, puts forward a completely automated process operated without any human intervention. Facial recognition, in this procedure, is used only to verify that the ID photo is of the same person as the selfie that is taken during the enrolment process. There are no further procedures to verify the true liveliness of the person. The automated process also involves an electronic signature on the contract for the banking product that is being offered, with an email sent that includes both the URL to direct the customer to their new user space and the username that allows them access to it.

31 Legifrance: CNIL informed decision n°2017-251 dated September 14th, 2017 about Société Générale.
32 Legifrance: CNIL informed decision n°2018-051 dated February 15th, 2018 about Boursorama.

On the subject of online-only identification procedures, we should take note of ANSSI's position. Within the framework of what eIDAS would categorise as either "substantial" or "high" identification security processes, when identity is validated remotely without the potential customer being present at the site of verification, a physical, face-to-face identity check equivalence is needed. This is done by setting up technical and organisational measures which fight against the risk of fraud and which are at least as reliable as physically showing ID and allow companies to cover risks linked to manipulation by simulating the real, physical presence of the person

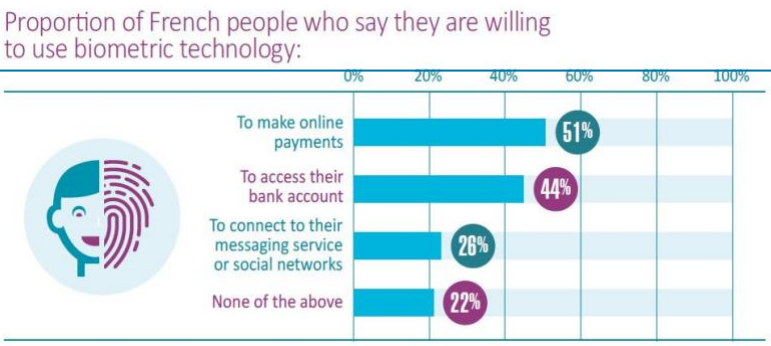
BIOMETRICS

In the words of CNIL, "biometrics brings togetherr all the different IT techniques which allow one party to automatically recognise an individual by his or her physical, biological or even behavioural characteristics." GDPR requires three prerequisites for the use of biometrics:

- A legitimate and lawful purpose: the equipment will only be validated if it meets a need for strong security;
- A prior consent: a specific (for the use in question), free (an alternative must be offered) and informed (explicit) consent from the user. In all cases, users retain the right not to give or to withdraw their consent at any stage of the process and to opt for a traditional alternative;
- A CNIL approved Privacy Impact Assessment (PIA). CNIL's standard position is to require encryption of the biometric minutiae.

The use of equipment which uses biometrics has expanded exponentially in France over the last few years: between 1978 and 2004 only 37 examples were examined by CNIL, whereas 800 authorisations were granted in 2017.

This growth is also reflected in the French public's evolving perception of biometric systems. The traditional mistrust of this type of technology is now tending to evaporate.



CIAM - A new approach to bring a unified and secure customer vision?

Customer Identity and Access Management (***CIAM***) solutions aim to combine the user experience and the needs of security in the best possible way, by reorganising a company's IT systems. Indeed, this type of solution allows a company to manage the entire user life cycle securely, while still offering a unified customer vision as it can process personal data in a centralised space. For banks, CIAM is the chance to eliminate data silos, by bringing together all of their customers' personal data, whatever its use may be (*account management, loans, insurance, etc.*). This CIAM approach can thus enable banks to offer customer relationship management which complies with GDPR as it satisfies the principle of privacy by default, whereas most CRM tools on the market cannot.

APIs, the banking world's "lingua franca" for the open banking age?

The protection of banking data is facing new challenges with the birth of the open banking era. This phenomenon is transforming the banking landscape, introducing new players, establishing new rules of the game and changing both codes and usage relating to banking data, which had previously been protected. Indeed, this new banking strategy is founded on transparency and sharing data between firms in the same ecosystem in order to provide richer services to customers. PSD2, which establishes a regulatory framework for this trend, requires the use of secure communication interfaces for this data sharing. Banks must therefore provide these interfaces for any third-party payment service providers (or TPPs) willing to access a customer's account data or to initiate a payment (e.g.). PSD2 requires the exchanges between these actors to be standardised and secured, via **APIs**.

API

An Application Programming Interface - API - refers to a general, normalised group of classes, methods and functions used in order to organise access to services,

resources and data for third-party apps. These interfaces have to be scalable, reusable and secure, all whilst offering simplified use and ease of integration to IT developers[33].

At present, the traditional methods of third-party service providers are based on the technique known as **web scraping**[34], which presents a risk to the bank in the form of the possibility of their website being slowed, or even brought to an outage, when there are too many requests to handle. In addition, web scraping does not guarantee a proportional use of a customer's data, nor does it comply with the principle of data minimisation. With it, when a TPP gains access, albeit with consent, that provider can recover all the information available about the accounts, including balance, transfers, withdrawals and all the metadata associated with it (place, date, time, company, amount, rental amount, repayments, loans, customer habits, etc.). Setting up secure interfaces which manage access to customer data is therefore a challenge that is likely to increase trust amongst customers towards their bank.

3.2. New services putting the emphasis on trust

Firstly, we should mention digital identity services, the cornerstone of trust in the digital world. With the explosion of passwords for customers to remember and laborious enrolment procedures, digital identity solutions aim to improve the user experience by enabling service providers (merchants) to take advantage of a prior enrolment carried out by an identity provider. Today, different solutions of this type co-exist, providing differing levels of guarantee. By relying particularly on secure enrolment for their customers via KYC processes, banks are able to provide digital identity services with a high level of guarantee.

Their legitimacy rests upon two further pillars:

- The high rate of banked people in France allows the banking sector to cover a large majority of the French population. This coverage would consequently encourage a large number of users to sign up for the launch of any potential digital identity services. If there is a large number of registrations, any service providers would logically prefer to rely on this service to sign up their users;

33 *API: this definition comes from the White Paper, "PSD2 and Open APIs: Threats and Opportunities for the banking sector. Are we moving towards Open Banking?" created by Galitt in partnership with DS Avocats.*

34 *Web scraping is a technique for extracting content from a website via a computer script or program which reads the html code, with the aim to use it in a different context.*

- The frequency of the customers to connect to their personal home banking proves that they are used to authenticating via their bank. This leads one to believe that customers would sign up to an electronic means of identification provided by the bank to grant access to other services.

By positioning as identity providers (*ensuring 3 processes: identification, delivery of the electronic means of identification, authentication check*), banks could strengthen their position as an everyday trusted partner in their customers' lives. This would also reinforce their image as a trusted third party, while allowing them to provide other related digital services (*secure messages, digital safes, electronic signatures, etc.*). On the other hand, not getting involved in this sector means a risk of seeing other parties establishing as the reference in providing digital identities, which could lead to them encroaching on the banks' customer relationships or even start to compete with the banks to offer connected services to their customers.

For a bank, becoming an identity provider is a strategic choice as it is at the heart of customer relations. It could also be a profitable choice, depending upon the business model put in place. A bank can opt to offer an electronic means of identification for its own customers or for its key partners (*as part of a single sign-on offer*) and all this without belonging to a federated identity system. Being part of a federated identity could be a significant asset if the identity platform is named by a European government as an eIDAS European node, as this would enable the identity provider to expand its offer to a Europe-wide scale. The service provider (*who does not know which identity provider the user has selected*) can pay for the ecosystem in order to take advantage of the solution, and then pay for each connection to the site (cost per use).

This federated identity solution lets a bank pool the costs of having identification and authentication solutions that comply with eIDAS, PSD2 and AMLD4. Finally, by joining this type of ecosystem, the bank can further strengthen its position as a legitimate trusted party.

Please note that the opposite path - that is, neglecting the digital identity field - can also result in an economic calculation which must be highlighted. Delegating the management of personal data to a third party can help a bank reduce its expenditure on the secure processing of customer data (*collecting, checking, storing, etc.*) and also on the costs of GDPR compliance. However, this short-term

view could be dangerous for a bank in the long-term, when considering the very vigorous international competition and the current swift development in digital technology and usage.

BUSINESS MODEL FOR ELECTRONIC IDENTIFICATION SCHEMES - THE EXAMPLE OF SPID, FROM ITALY

The eIDAS European regulation requires official notification of national electronic identification programmes at a European level. The objective is to strengthen user trust and to widen the boundaries for using the solutions by enabling mutual recognition between member states of the identification means used by the different recognised schemes. Amongst those nations which have notified the European Commission of their electronic identity programme is Italy, with the introduction of SPID[35]. With SPID, a service provider can obtain the ID data required to authenticate their users, based on a verified identity set by the Italian programme. For authentication, the billing model proposed by the identity providers working within the framework of the SPID programme is described in the following table[36].

Offer	Number of users included in the offer	Fixed cost (per user)	Cost per extra user
Unit price	0	0€	€1.20
Small	50,000	€50,000 (€1)	€1.20
Medium	250,000	€200,000 (€0,80)	€1
Large	500,000	€300,000 (€0,60)	€0.80
Extra Large	unlimited	€800,000	n.a.

In Europe, several companies provide or help provide digital identity solutions. Asquared, a consulting company, published a list of these companies in February 2018[37].

35 *The Italian electronic identification programme's website, available in Italian and German.*

36 *These fees, offered in September 2017 by identity providers, may have changed since then.*

37 *Asquared, E-Identity Solutions in Europe - A European overview, February 15th, 2018.*

Amongst these companies appear several banks. Some deliver what are called "Mobile ID" services which offer:

- Mobile identification solutions (eKYC), the alternative to this new stage of identification could be to dematerialise a piece of ID onto a mobile phone (the lifecycle of this mo- bile identity would be therefore strictly linked to that of the original ID document, and it would be managed by the same provider as that document);
- And/or mobile authentication solutions. One example of a mobile ID solution established by major banks is the one set up by the Belgian itsme® consortium.

INTERVIEW

John Van Der Heyden

Sales and Personal Banking Director of BNP Paribas Fortis Belgium

What exactly is itsme®?

In Belgium, the mobile phone operators and the banks have joined up to create a reference in the field of mobile identification and in terms of privacy in the digital world: itsme®. Thanks to this mobile app, every Belgian citizen can **identify** themselves unequivocally when they sign in to digital apps, to **confirm** *(payment)* transactions and even to **sign** official documents.

The itsme® app is universal and allows users to have a single password to sign in. In this way, customers can manage their data and banking operations simply. All they need to do is install the app, set up their itsme® account *(their digital identity)* and then to choose a five-digit code. For some operations, it's even possible to use biometrics, depending on your model of smartphone.

The opportunities for using itsme® are endless: you can easily register as a new customer with a bank or a merchant, you can request an official document from your town hall, you can check the details of your insurance policy online, you can sign payment transactions with "Easybanking", in the future, you could also - why not? - secure your home or turn on the heating remotely *(with the Internet of Things)*. As of January 2018, the itsme® mobile identity app is officially recognised by the government. Feedback from the app has been extremely positive. In just over a year, more than 500,000 Belgians have already embraced it.

How did you manage to successfully combine it with your bank's services?

Fortis doesn't force its customers to use itsme®. They could just as equally use the procedures that the bank had already put in place. These haven't been changed. So, there's no overlap between the use of itsme® by customers and the bank's business. It's simply an extra service for its customers.

What advantages can the bank take from this partnership?

Fortis has two connections to itsme®. We are a member of the ecosystem, as an identity provider and a user of the means of authentication that itsme® offers. Thanks to the customer identification procedures *(KYC)* that the bank is legally obliged to set up, the bank already has the verified identities of all its customers. When a user wishes to create their itsme® digital identity, they can do it using the verified identity held by the bank.

Today, almost all banks offer an authentication and signature service via their mobile app. This service, in itself, isn't something that helps a bank stand out from its competitors and it is hard to make it profitable. However, creating a single sign-in service across all the banks allows them to develop their services much more quickly and introduces economies of scale. The itsme® project transforms an expense into a saving and will potentially become a source of revenue in future years.

How do you manage the effects that using such an innovative solution can have, when it comes to issues of security?

The app offers a triple security lock: itsme® only works with the correct combination of smartphone, SIM card and personal itsme® code. itsme® not only enforces the European electronic ID regulation *(eIDAS)* and the General Data Protection Regulation *(GDPR)*, but also the rules of Strong Customer Authentication *(SCA)* set out in PSD2.

In addition, users' personal data is stored in a kind of "safe" held by itsme®, which is ISO 27001 certified.

What is your strategy for the next five years? What further improvements can be brought to the itsme® app?

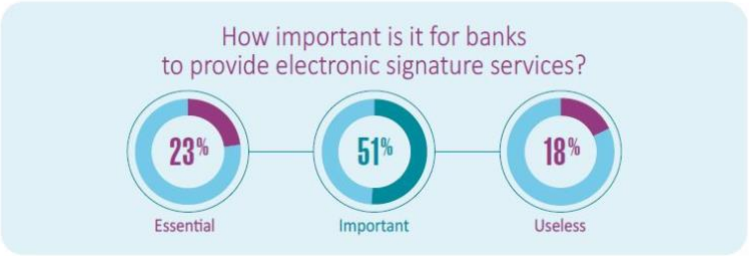
Immediately upon its launch, in May 2017, itsme® already offered 3 of the 4th features that we wanted to get onto the market: sharing verified identity data, signing in and confirming payments or orders. The 4th feature is the certified electronic signature. We are currently working on the development of the solution, and we are waiting for European certification of the service.

By now, almost the entire banking sector has joined itsme®. Other fields haven't remained inactive either, for example private insurance, auction sites, real estate and health insurance.

We also have international ambitions: itsme® will be crossing the border into Luxembourg. itsme® has had a wonderful start in Belgium, which we are really happy about, but we believe that the product still has the potential for much more, including outside our borders. That's why Belgian Mobile ID signed a strategic partnership in May 2018 with LuxTrust to position itsme® in the Luxembourg market.

Electronic signatures

Electronic signatures are electronic proof delivered by a person to confirm their agreement with the content of a document or set of data linked to the signature. It involves guaranteeing the authenticity and integrity of the document as part of an operation or transaction between two parties, as well as ensuring the identities of the signatories with the help of the electronic signature certificates. Electronic signatures can be used as an electronic dematerialisation of the hand-written signature with greater or lesser probative value, depending upon the type of signature and certificate[38]. Only the qualified signature provided by a qualified trust service provider (QTSP) has the same value as the hand-written signature, and this has Europe-wide interoperability. Other levels of either simple or advanced signatures can benefit from the principle of non-discrimination, but it's up to the bank to prove the signature's value within the national jurisdiction of the customer[39]. A majority of French people view this as an important service for banks to provide.



Personal data sharing

The identity provider can, above and beyond the data required to identify and authenticate, recover some ancillary data from the user (for instance a tax return in the case of an offer of a long-term depreciable loan for a property). The provider will be able to transmit this to a third-party data provider, subject to receiving prior and explicit consent from the user and only for legitimate and proportional purpose. For the user, the benefit is the ease of use when dealing with service providers which require specific data.

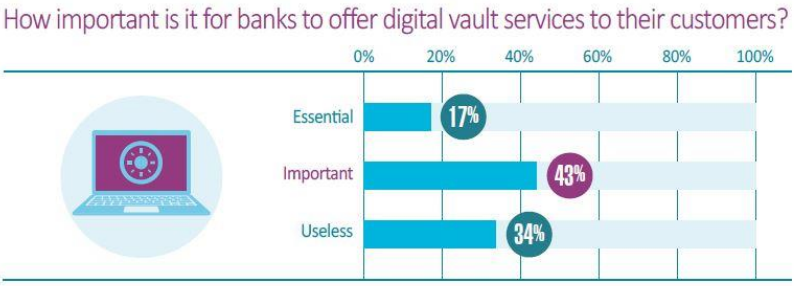
38 *For more information, consult the European Union webpage entitled, "What is an electronic signature?"*

39 *To learn more about different levels of signature, read the guide about archiving electronic signature proofs on the fly, from FNTC.*

The digital safe

Another opportunity for the banks to cash in on is the creation of secure digital safes which will soon be certified by ANSSI - Some are already offering the service to their customers. The banks have the technology, the know-how and the legitimacy needed to offer this type of service, especially given the trust and esteem in which they are held by French citizens. French banks have only recently been able to offer this type of service as the decree authorising digital safes was signed in 2018[40]. Digital safes allow banks to provide a very secure, trusted, digital space to their customers, who can use it to store digital items which are not necessarily connected to their bank data (e.g. bills, contracts, diplomas or photos). It also provides guaranteed confidentiality and integrity of the information held, while still offering easy accessibility for the user.

A majority of French citizens feel that digital safes are an important service for banks to provide.



Some of the opportunities mentioned in this section must, if a bank wants to maximise the potential added value, be offered to customers in combination with others. This is the strategy adopted by Docapost and Vialink, which have brought their respective fields of expertise to build a 360° KYC platform, combining digital identity, digital safes and machine learning[41].

These different ways, whether they deal with internal banking functions or offer new services, show that the banks are not short of alternatives if they want to reinvent themselves and strengthen the confidence their customers put in them.

40 *Legifrance: Decree n° 2018-418, dated May 30th, 2018, relating to ways and means in which a digital safe service should be set up.*

41 *Press release from Docapost and Vialink about the establishment of a single platform for total KYC identification, dated October 15th, 2018.*

Conclusion

The payment market is in a period of dramatic change, which can be shown by the wave of new European regulations that aim to make the digital world more secure, and thereby force change upon the banks. However, rather than see this as a constraint, the banks must seize it as an opportunity to initiate a reflexion on their business and the relationship they have with their customers. The latter are increasingly sensitive to security issues linked to digital practices. As an actor which benefits from its customers' confidence, a bank has some of the responsibility to strengthen security in the digital realm, by protecting its customers' personal data. Indeed, adopting this position enables the banking sector to grasp a double opportunity, both defensive and offensive: retaining its legitimacy as a trusted party, and developing new commercial directions.

To take full advantage of this opportunity, banks must not lose sight of their customers' expectations when it comes to offering an autonomous, smooth and personalised service. For this reason, a "customer in control" standpoint - for setting up services which deal with subjects as sensitive as processing personal data - makes perfect sense.

Allowing the customer control over the settings of a service is not a step into the unknown for banks, as they have been offering so-called "self-care" services for a few years now. These let customers regulate the settings for the use of their banking products via a mobile app or via their personal home banking account. On the other hand, extending this principle to a customer's digital identity is an avenue worth exploring in this reinvention that banks need to undertake. The current interest from customers in protecting their personal data naturally leads towards the adoption of such a service. In addition to digital safe services, which enable documents secure storage, banks could offer a platform of services to manage the various user rights and consents given by customers for the limited, or unlimited, use of their personal data.

A customer would be able, using a mobile app and having accepted to entrust the management of their digital identity to a third-party service provider, to configure access to their personal data. The customer could also set up different authorisations or restrictions of access to some categories of personal data. With this in mind, we can imagine a project from players in the banking sector to develop a platform of this kind using a shared infrastructure. The bank would then become the identity provider, in charge of processing their customers' personal data.

Beyond the advantages of such a step, in terms of customer expectations and the stakes in the digital world, banks have to see the current changes in their sector as an opportunity to become the essential actor for their customers in their digital lives, whatever the domain of activity.

About the authors

Nathalie Launay - *Regulatory Consultant*

After 15 years working with the leaders in cards and identities, Nathalie has consolidated her technical expertise with consultancy assignments for SMEs and a start-up, while sharpening her sector- specific and multi-sector regulatory knowledge. In 2018, she joined Galitt to help payment firms with their new digital usage, based around reliable digital identities and trust services.

Cécile Rouhaud - *Practice Manager - Benchmark Observatory*

Cécile is in charge of the quantitative consumer and professional surveying department. She is particularly involved in creating Observatories, such as the Mobile Payment and Contactless Observatory (OPAMSCO) and the New Authentication Modes Observatory (OMODA).

Gwendal Boëdec - *Payment Consultant*

A graduate of Rennes Institute of Political Science and the "Ecole de Guerre Economique" (EGE), Gwendal is currently a consultant within Galitt's Payment Consulting Business Unit, mainly working on subjects linked to innovation and regulation in the payment sector.

Oriane Perrachon - *Business Analyst*

The primary contributor to this white paper, Oriane has completed her graduation internship with Galitt, as part of her 2-year Master's at ISIT Paris.

Several other Galitt partners have contributed to this project:

Emmanuel Caron : *Practice Manager*

Nathalie Gaudin : *Practice Manager*

Rémi Gitzinger : *Executive Director*

Alexandre Martin : *Practice Manager*

Isabelle Pujadas : *Communication Director*

Rendre les paiements simples, efficaces et sûrs, dans la vie de tous les jours.

galitt
a Sopra Steria company

17 route de la Reine
92100 Boulogne-Billancourt- France
Tél. : +33 1 77 70 28 00
contact@galitt.com
www.galitt.com