BBVA | RESEARCH

Digital Economy Outlook

September 2015
Financial Inclusion Unit

- Economic issues regarding data protection regulation: How to regulate data privacy?
- Fast retail payments: A glance at pioneering European experiences
- Improving credit access for the “invisibles”: Alternative data for credit scoring
- E-money regulation in Colombia: A dicey step beyond transactional services
- Biometrics: The future of mobile payments

Index

Summary

Economic issues regarding data protection regulation

How to regulate data privacy? The digital era is characterised by the intensive use of data which nowadays is easily obtained through cyberspace. In many cases, this information is considered private while the owners are unaware of how their data was obtained and used. Although current regulations around the world deal with these issues, from an economic point of view there are still many challenges ahead under debate.

Fast retail payments

A glance at pioneering European experiences. Fast retail payment infrastructures are currently been developed in several European countries – including Spain – as well as at the pan-European level. They are vital to satisfy customers' new expectations within the banking system, ensuring payment security and financial integrity. Here, we take a glance at the pioneering European experiences in the UK, Poland, Sweden and Denmark, to see how their fast retail payment systems work.

Improving credit access for the "invisibles"

Alternative data for credit scoring: an opportunity for financial inclusion. By using alternative data that can predict credit risk and segment customers, more people could access financial services at a lower cost while reducing the risk of lending and borrowing in informal markets. It helps people with limited financial information to access credit by building a credit risk profile.

E-money regulation in Colombia

A dicey step beyond transactional services. The new regulatory framework allows non-bank entities to offer electronic deposits under a simplified financial license. These deposits are covered by the Deposit Guarantee Fund and are not subject to amount limits, going beyond the transactional purpose of e-money services. This may pose some risks if new players are not properly supervised.

Biometrics

The future of mobile payments. The multiplication of threats from security breaches has prompted more advanced methods of authentication and verification, such as biometrics. For banks and customers, the use of biometric authentication delivers significant benefits: boosting security and trust, enhancing the customer experience and improving efficiency. Biometric authentication will continue to grow at a fast pace, creating new business and employment opportunities, while transforming payment and non-payment transactions.

1 Economic issues regarding data protection regulation

How to regulate data privacy?

The digital era is characterised for the intensive use of data which nowadays is easily obtained through cyberspace. In many cases, this information is considered private, while the owners are unaware of how their data was obtained and used. Although current regulations around the world deal with these issues, from an economic point of view there are still many challenges ahead under debate.

Personal information in the digital era

Issues related to the protection of personal information - also known as data protection - are not new. In fact, this has been contemplated for quite some time in international and domestic legislation as part of basic Human Rights. Practically, all countries consider the right to privacy in their constitutions.

However, during the last three decades the topic has been of increasingly relevant concern, hand-in-hand with the development of the digital era. Thanks to the exponential increase in processing speed, computing storage and the consequential ramifications of mobile technology - 'Big Data' analysis, networking and retail services - the issue of private information circulating in the cyberspace becomes fundamental.

The topic of how to regulate personal data is important because it has the potential to provide benefits to firms and customers in different economic sectors. For instance, data containing personal characteristics has the power to personalise products and services as well as to make a variety of production processes more efficient, adding value to the interaction of supply and demand. However, alongside the benefits, there are costs to be taken into account, and this is why a good regulatory framework is a keystone.

The economics of personal data

Personal data can be traded in the market. People who hold the information could be considered the supply side while firms, willing to use the data, are the demand side. As a consequence of network externalities, derived from an increasing participation of economic agents which are more and more interested in obtaining benefits, this potential market is growing, with enormous costs and benefits that could be extracted from them.

Web-based retail business and the digital social networks (e.g. Facebook, Twitter and others) are examples of this growing interaction, where people and firms are directly gaining from the relationship; as well as all the collateral consequences of data-mining using algorithms, offering more products in different retail industries. The issue, notwithstanding, is that both sides of the market – or at least one – could not be completely aware that this market exists and/or how it works, and that their personal information could be used and passed from one hand to another. This and other elements are some of the relevant market failures that need to be tackled.

Market failures to overcome

A market failure is a condition that limits the adequate functioning of the market, blocking the possibility of obtaining the maximum value for society. One of the most complicated failures that this potential market for personal data has to cope with is, precisely, the lack of adequate explanatory information, especially for those who are the owners of their private data. First, people interacting with web pages or applications are not aware of the use of the information they provide and the consequences this has for them. Even more, in cases where firms give notice about the use of the information or ask for permission for using it, owners of the data do not spend time to read the warnings. Privacy policies seem to be complicated and hard to

understand for the common citizen. Moreover, until now, there have been no available adequate metrics for measuring the real benefits or costs that this market is bringing to consumers, which makes things more difficult to understand.

Other market failures are related to issues of data security, with concern over the capacity of firms – whether large or small - to safeguard the information in order to avoid data breaches that could dent confidence in this market. Other problems are those of competition, where digital giants stand as dominants in the market with likely effects on current (or shadow) prices of information. Last, but not least, are those inefficiencies imposed on the market by inadequate regulation, many times as an unintended bad consequence of good intentions. As the theory of economic regulation states, not all public intervention is adequate or even necessary for reaching market efficiency.

Paving the way for future regulation

Different studies highlight that regulating the market for personal data needs to provide better control for owners of their data, allowing them to offer or restrict their information depending on their preferences. For this to happen, it is crucial that regulations standardise and simplify privacy policies.

Current formats for acceptance of, and consent to, the use of personal data should be straightforward, swift and easy to understand. Some studies propose the creation of a profile of the acceptance of the use of personal data which is conducted only the first time, and which can then be used by any company or ITC application in the world, thus bringing down the transactional cost to the economic agents who have to obtain authorisation every time they request access to the data.

Another approach could be to allow greater control over the individual's own data, by means of mechanisms which enable them to decide how their data will be managed, throughout the life of the contractual relationship, which would add greater transparency and could generate trust.

However, some experts think that to transfer all responsibility for how personal data is used to the owner is unfair, because the matter is complex and it is very unlikely that they will understand all the consequences involved when their personal information is available in cyberspace. Some suggest shifting the weight of responsibilities to those firms using the information, given that they know much better than anyone else – and definitely much more than the consumer or the regulator - the intended consequences of using the data.

In order to get a better balance of responsibilities, it would be reasonable to discuss the possibility of introducing the role of "algorithm monitors", scientists who audit algorithms, in the definition of the regulations and in the design of supervision over personal data. This would create a fair balance between the individual on the one side and the benefits to society in terms of information use on the other. Society should use this type of specialist to certify how data is used through the creation of professional bodies of algorithm monitors, subject to strict conduct and ethics codes in their activities.

Finally, for the design of appropriate regulation, it is fundamental to keep in mind the issue of generational transformations of societies. Recent studies have been confirming that the perception of what is private or not, and what information should be shared, is changing across different generations. We are able to see this for ourselves when we interact on social network platforms. According to these studies, people are more willing to trade information that could previously have been considered private by older generations and, at the same time, there is more market demand for these data. However, the sluggishness of the regulatory framework to adapt to this moving context is probably creating inefficient consequences for the economies.

2 Fast retail payments

A glance at pioneering European experiences

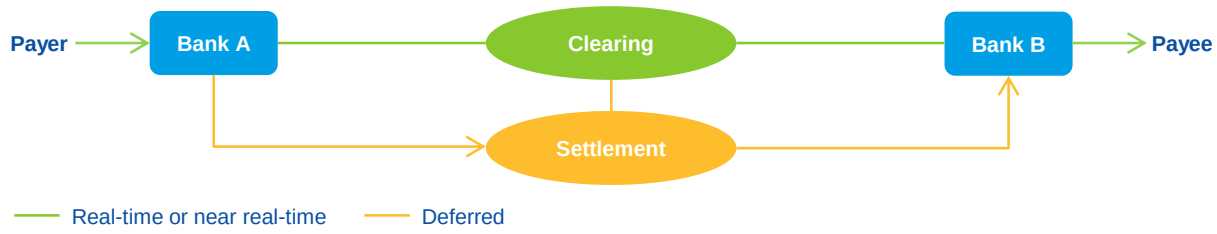
Fast retail payment infrastructures are currently been developed in several European countries – including Spain – as well as at the pan-European level. They are vital to satisfy customers' new expectations within the banking system, ensuring payment security and financial integrity. Here, we take a glance at the pioneering European experiences in the UK, Poland, Sweden and Denmark, to see how their fast retail payment systems work.

What really does take place in real time?

Fast retail payments refer to fund transfers (i.e. account-to-account payments initiated by the payer) in which the funds are posted to the beneficiary's account in near real-time 24x7x365. This involves the payment clearing (i.e. the validation of the instruction between the payer's and the payee's banks) taking place immediately after the transfer has been authorised by the payer. Yet settlement (i.e. discharging banks' obligations through the transfer of funds) may take place at a later time. Indeed, fast retail payments sometimes rely on the pre-existing deferred net settlement systems, such that the transfer of funds between banks takes place only a few times per day in central bank money. Therefore, in many cases, the so-called fast retail payments are immediate for end users, but not from the banks' perspective.

In retail payment systems with immediate clearing and posting but deferred settlement (see Figure 1), banks face the credit risk arising from making funds available to payees before payments have been actually settled between banks. This risk can be mitigated in different ways: by capping the banks' net settlement positions, requiring banks to collateralise or pre-fund their positions or shortening the settlement cycles.

Figure 2.1
Fast retail payment systems with deferred settlement



Source: BBVA Research

European pioneering systems

The UK (*Faster Payments*, 2008), Poland (*Express Elixir*, 2012), Sweden (*BiR*, 2012) and Denmark (*Straksclearing*, 2014) have all launched fast retail payment services, which coexist with the existing deferred systems. In the four countries, the new systems are near real-time from the end users' perspective, but differences arise in the settlement mechanisms and the associated banks' guarantees:

- **UK**: deferred net settlement (three cycles per day) through accounts held by banks at the central bank. To mitigate settlement risk, net debit positions are subject to a cap and have to be partially collateralised, as part of a liquidity and loss-sharing agreement between member banks. This will be replaced by a new model in which each bank fully pre-funds its maximum debit position with cash.
- **Poland**: prefunded settlement by the clearing house based on an escrow account in the central bank.

- **Sweden**: real-time settlement by the clearing house using prefunded special accounts that are backed by an escrow account in the central bank.
- **Denmark**: deferred net settlement (six cycles per day) via the settlement accounts held by banks at the central bank. The system is pre-funded as the liquidity available in a bank's settlement account determines its maximum debit position in the system.

Satisfying customers' demands within the banking system

In those pioneering countries, upgrading the banks' payment infrastructure has fostered the emergence of innovative mobile-based payment solutions that satisfy the customers' demand for immediate and seamless payments. Meeting that demand within the banking infrastructure guarantees secure and safe payments and ensures the integrity of the financial system.

3 Improving credit access for the "invisibles"

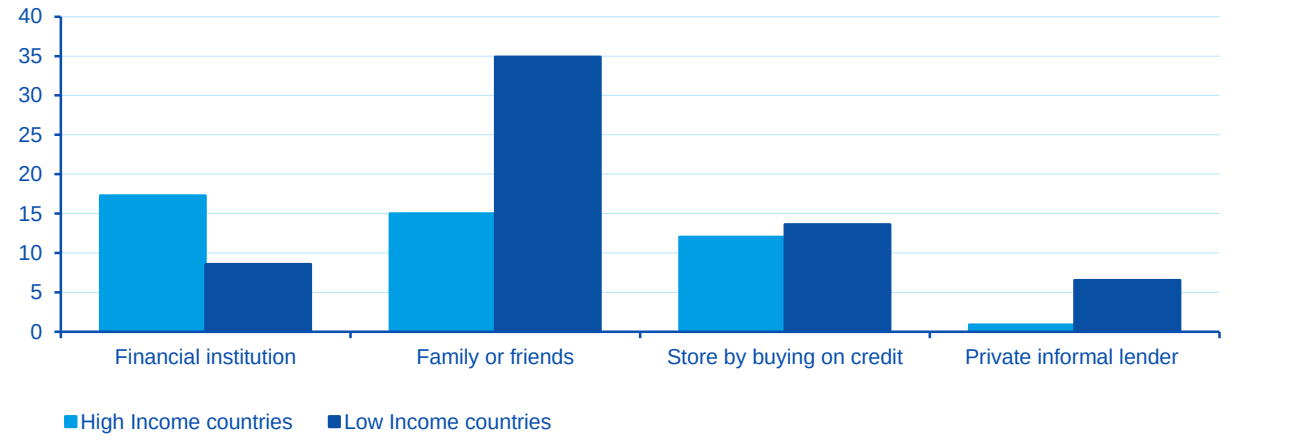
Alternative data for credit scoring: an opportunity for financial inclusion

By using alternative data that can predict credit risk and segment customers, more people could access financial services at a lower cost while reducing the risk of lending and borrowing in informal markets. It helps people with limited financial information to access credit by building a credit risk profile.

How do people borrow?

When asking adults in a population if they borrowed any money in the last year, regardless of the amount (yes/no question), one finds some differences by comparing different income group of countries. According to the Global Findex (2015), 38% of the adults in high-income countries have borrowed money in the last twelve months, whereas for low income countries the figure is 52% (47% and 38% for lower and upper middle-income countries respectively)[1]. However, differences are negligible in the percentage of people who borrow between the richest and the poorest within these groups. Dramatic differences arise when asking for the sources of borrowing. As illustrated in Figure 1, the patterns followed by high and low income countries are different. While for high-income countries the main sources of borrowing money are financial institutions, the most important one for adults living in poor countries is informal. 35% of people who borrow money in poor countries do so from family or friends, and only 15% use this source in high-income countries. Also, adults in low income countries use private informal lenders seven times more than their counterparts in high-income countries.

Figure 3.1
How do people borrow?



Source: Own elaboration with Global Findex (2015) data, World Bank

The conditions for accessing formal credit are hard to meet for people without a detailed credit report or credit score. These people, who are "invisible" to the financial system, face several problems when it comes to managing their personal finances efficiently. In this scenario, high-cost lenders such as pawn shops, pay-day lenders, family and friends fill the void. This matter raises the issue that accessing credit may not be contributing to reduce the income-gap and inequality.

1: It is important to keep in mind that the way in which the survey question was asked (and its respondents) will influence the answer. For example, the Global Findex survey asked whether, in the past twelve months, the respondent had borrowed any money from any of the listed sources. People may have forgotten or deliberately withheld information on outstanding loans taken out more than twelve months prior.

Alternative credit scoring

Although interest in developing stable credit reporting systems is growing (the number of credit bureaus around the world between 1990 and 2011 is estimated to have tripled according the FI2020 Roadmap on Credit Reporting) most of the existing mechanisms have not succeeded in reaching base of the pyramid. Credit bureaus only report negative information from a prospective client, which does not solve the problem of assessing credit risk of someone who has a pattern of good behaviour or has no credit information. This asymmetry of information between those who want a loan and financial institutions is what prevents the financially excluded from accessing formal credit on good terms.

Providing alternative data for credit scoring is an opportunity for financial inclusion when it comes to credit. Particularly, a large number of people can benefit from accessing credit at effective conditions. A growing number of companies are using non-financial services data such as energy utilities, telecoms and cable TV history and rent to determine credit worthiness and to reach clients that typically would be financially excluded, not because they have a high associated risk but because they are "invisible". Including data on cell phones and TV, apart from utilities, provides excellent credit-rating value since empirical analyses show that these data are much more sensible to household income shocks.

By using alternative data that can predict credit risk, more people could access financial services at lower cost, while reducing the risk of lending and borrowing in informal markets. It helps people with limited financial information to access credit by building a credit-risk profile based on their payment behaviour outside the financial system. Since almost every household in the world needs to deal with utility bills such as electricity, water, gas or mobile phone, it is straightforward to take advantage of this behavioural information to help in the prediction of individual credit risk, and to make "visible" those without enough information to be credit worthy. Alike, this information helps loan-givers to expand their assessment models.

Thus, alternative credit scoring adds value to both users and the financial sector. On the one hand, users can demonstrate that they are good payers, increasing their chances to get credit on better terms. On the other hand, banks have more relevant and objective information of the payment behaviour of their prospective clients, which helps in reducing the default rate and increases their customer base.

Case study: evidence from Latin America

Although the use of alternative credit scoring is not new, *Destacame* is the first behaviour-based credit score in Latin America, and also the first platform that allows users to own their information and use it for their own benefit. This platform gathers historical payment information, uploaded by the individual, from utility companies and using a unique algorithm it creates a credit score. For instance, when a person asks for a loan or post-paid plan for their phones, *Destacame* sends his/her score to the bank/retailer or telecommunication company, who will pay for the information and use it to improve the credit risk assessment system that they have in place. The service is free for the borrower. With a target market of people located in the middle to lower part of the income pyramid (mainly those that currently have no (or limited) access to credit), this is a good initiative to improve financial inclusion. It has a different strategy from that of credit bureaus, because the latter have access to the information of those that do not repay their loans directly through lenders. Not being in this database does not necessarily mean that the person is a good payer, which limits the predictive capacity of their data. Also, credit bureaus still do not have each person's consent to access the way they pay their bills, nor their trust.

4 E-money regulation in Colombia

A dicey step beyond transactional services

The new regulatory framework allows non-bank entities to offer electronic deposits under a simplified financial license. These deposits are covered by the Deposit Guarantee Fund and are not subject to amount limits, going beyond the transactional purpose of e-money services. This may pose some risks if the new players are not properly supervised.

The October 2014 law

In October 2014 the Colombian government enacted Law No. 1735, creating a new type of financial institution – Specialised Companies in Electronic Deposits and Payments (SEDPEs by its Spanish acronym) – that, under a simplified financial license, are allowed to raise funds from the general public through "electronic deposits". This product had already existed in the Colombian financial system since 2011, but its provision was restricted to credit institutions. The new law allows the SEDPEs to offer electronic deposits with the same features as those offered by banks, i.e. deposits may be remunerated and are covered by the Guarantee Fund for Financial Institutions. However, as the SEDPEs are not subject to the same regulation and supervision as banks, they are not allowed to conduct financial intermediation and must hold 100% of the funds raised in overnight deposits either at commercial banks or at the central bank. The law also establishes that the SEDPEs fall under the supervision of the financial watchdog (*Superintendencia Financiera*) and must hold a minimum capital of 5,846 million pesos (roughly 1.66 million euros) – a figure which is revised annually according to the CPI.

Second-level regulation

The October 2014 law mandated the government to establish additional financial requirements for the SEDPEs, as well as to define the limits and 'know your customer' (KYC) requirements of electronic deposits. The government did so on 13 July by Decree No. 1491, which establishes a prudential capital requirement for the SEDPEs of 2% of the funds raised. Regarding electronic deposits, the decree establishes two different categories: one with a simplified account-opening procedure (no physical presence required) but subject to limits for balances and debit transactions per month (three monthly minimum wages), and another one with the standard KYC requirements and AML/CFT procedures but which is subject to no such limits. This was particularly surprising, as the draft decree released by the government in March 2015 also set limits for the deposits with standard opening procedures; only special electronic deposits for payment collecting purposes were not subject to limits.

Colombian regulation in the Latin American context

As shown in Table 1, there are several aspects in which Colombia differs from the general regulatory approach: i) electronic deposits may be interest-bearing; ii) they are directly covered by the deposit guarantee scheme, and iii) they are not subject to amount limits when the standard KYC procedures are applied.

Table 1
Comparison of the e-money regulatory framework in Latin American countries

	Colombia	Paraguay	Peru	Uruguay
Prudential capital requirement for non-bank issuers	2%	No	2%	No
Limits to balances and transactions	Only for simplified accounts	Yes	Yes (standard accounts: only limit to transactions)	Not specified
Interest payable on deposits	Allowed	Not allowed	Not allowed	Not allowed
Deposit guarantee scheme	Yes	No	No	No
Type of assets in which non-bank issuers must hold the raised funds	Bank deposits	Bank deposits	Bank deposits, government securities (up to 30%) or other authorised liquid assets	Bank deposits, government securities or other authorised liquid assets

Source: BBVA Research

Opening the e-money business to non-bank institutions, such as mobile network operators (MNOs), has the potential to reach the unbanked population more rapidly, leveraging the MNOs' infrastructures and customer bases. However, given the simplified licensing of non-bank players as well as the transactional purpose of e-money, there should be amount limits for balances and transactions, as is the case in most of the e-money regulations worldwide. Otherwise, risks may arise if non-bank institutions are not properly supervised.

5 Biometrics

The future of mobile payments

The multiplication of threats from security breaches has prompted more advanced methods of authentication and verification, such as biometrics. For banks and customers, the use of biometric authentication delivers significant benefits: boosting security and trust, enhancing the customer experience and improving efficiency. Biometric authentication will continue to grow at a fast pace creating new business and employment opportunities, while transforming payment and non-payment transactions.

Security

The increasing usage of Internet, mobile devices, Wi-Fi, and cloud computing continues to expand the frontier of products and services available to billions of people around the world, with the potential to significantly enhance well-being even in the most remote areas of our planet. However, this has also multiplied the threats from security breaches, prompting more advanced methods of authentication and verification such as biometrics. Over the past few years, cyber-attacks have grown in size and virulence, reaching critical industries such as banking, utilities, and airlines, as well as other sectors like retail, entertainment and hotels. In addition, the attacks have targeted governments and the military, escalating national security concerns. The damage includes job losses as the economy diverts resources to activities that provide lower value, disincentives to innovation by eroding the returns on intellectual property, and destruction of commercial activities due to losses of confidential information and market manipulation. In addition, the economy suffers from higher opportunity costs or reduced value-added from foregone activities as a result of lower investment in R&D, higher spending on network defenses and risk-averse behavior from consumers and businesses. Moreover, cleaning up cybercrime can reach significant amounts, particularly when the damages affect the brand, reputation and, customer retention and satisfaction.

According to the Center for Strategic and International Studies (CSIS), the cost of cybercrime to the global economy is around $450bn. Moreover, the Ponemon Institute reports that in 2013, 43% of U.S. companies experienced a data breach. At the individual level, the biggest risks are identity theft and loss of confidential information. The CSIS estimates that, in the same year, there were 800 million individual records stolen around the world. In South Korea, for example, more than 70% of individuals aged 15 to 65 years had their personal data stolen and credit cards compromised in one month. In the U.S., according to a 2012 survey from the Bureau of Justice Statistics, identity theft affected 16.6 million people with a cost of $24.7bn in financial losses.

Biometric banking

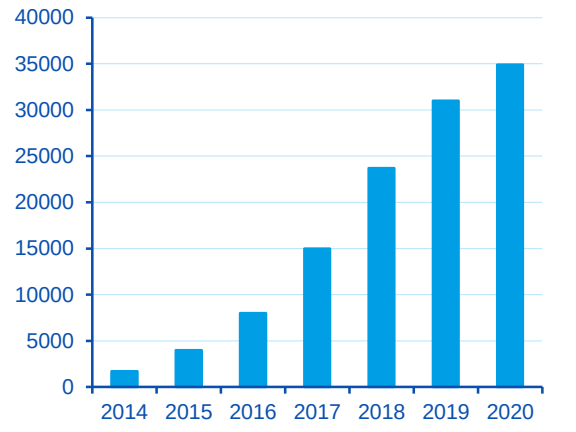
In response, a wave of innovation and capital has centered on developing new technologies to protect individual data and enhance customer experience. One option that is growing at a fast pace and shows great potential is biometric authentication. In essence, biometrics uses physiological and behavioral characteristics like DNA, fingerprints, eye retinas and irises, voice patterns, facial patterns, vein and signature patterns and hand measurements for the purposes of authentication and verification of human beings.

Despite elevated uncertainty on how the biometric market will evolve in the next few years, expectations are positive. For example, Acuity estimates that by 2020, biometrics will be used to authenticate almost 65% of all mCommerce transactions. In addition, global mobile biometric revenues are expected to increase to $34.6bn from $1.6bn in 2014, with 35% being authenticated via mobile devices and 65% via apps downloaded by consumers. Other estimates indicate that the global biometrics technology market will reach

$22bn by 2020, up from $11.2bn in 2015 and $4.2bn in 2010. In the financial sector alone, the market value could reach $8bn by 2020[2]. This includes biometrically-enabled smart mobile devices, biometric sensors, biometric app downloads, direct purchase and software development fees, and authentication fees from biometrically secured payment and non-payment transactions.

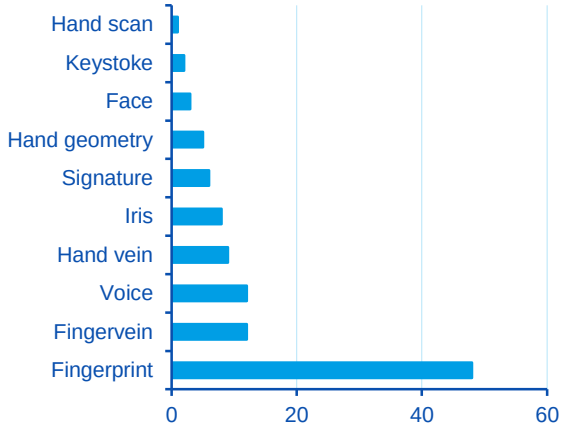
Biometrics is not uncharted territory for the financial industry; banks have explored options such as fingerprint scanning for decades, but the convenience and proliferation of mobile devices is making biometrics accessible to anyone with a smartphone. Fingerprint recognition has historically been the preferred option in the financial sector given its high accuracy and low-cost. A 2012 survey among 121 banks using biometrics revealed that 48% prefer this technology. Nonetheless, other technologies that fall under the contact less category, such as voice, iris, vascular and facial recognition are gaining ground and will provide greater versatility and convenience. In any case, this implies that the era of physical –cards- and logical –PINs and passwords- security measures may soon be over; providing the opportunity to develop a more integrated environment, where users can easily access a multiple range of products and services in a seamless fashion.

Figure 5.1
Mobile biometric revenue (USD millions)



Source: Acuity

Figure 5.2
Use of biometric technologies among banks (%)



Source: Biometix

Benefits and Challenges

For banks and customers, the usage of biometric authentication delivers significant benefits. First, it provides competitive advantages as better security increases trust, which represents the backbone of the business model. For example, biometrics can strengthen proof of identity processes, enhance fraud detection and improve identity management. Second, biometrics boosts customer experience by simplifying access, speeding processing times and facilitating a multichannel environment. Third, the combination of biometrics and other technologies can improve transparency, data analytics and real-time risk assessment. Finally, biometrics increases efficiency by lowering costs, improving internal controls, and facilitating audit trails and regulatory compliance. For example, biometrics provides an efficient way to comply with Know-Your-Customer requirements, which are aimed at curbing identity theft, financial fraud, money laundering and terrorist financing.

2: See for example MarketsandMarkets, 6Wresearch and Visa.

The increasing adoption rate of biometrics in the financial sector seems inevitable. A survey from Telstraglobal on Generations X and Y (born 1966-76 and 1977-94, respectively) indicates that more than half of respondents value trust as the most important driver of choice when selecting a financial services provider. One in five individuals would share their DNA to help secure financial and personal information, while up to one in two are willing to pay for mobile identity. In addition, less than half are satisfied with their institution's security performance, more than a third have experienced identity theft, 40% of victims believe it was the institutions' fault, and 65% of them are likely to defect as a result.

Biometrics in banking is most popular in developing economies in Asia, such as India and Indonesia. In fact, this continent accounts for 52% of banks using biometrics worldwide. The Americas ranks second with 32%, followed by Europe (9%), Africa (6%) and Australia (1%). Across industrialized countries, Japan ranks at the top supported by a network of over 80K biometric ATMs and more than 15 million customers. These differences may reflect higher regulatory hurdles in the U.S. and Europe, associated with strict personal data protection rules.

Moreover, financial institutions and regulators in advanced economies have been cautious to implement biometric authentication as litigation costs and other damages caused by information leakages in centralized databases could be devastating, particularly if security breaches compromise operations in other industries or government agencies. For example, after an attack occurs, banks can issue new credit cards but are obviously not capable of replacing fingerprints. Likewise, if a credit card is compromised the damage is to the customer and the bank. However, if biometric information is hacked, it can be used on a wide range of activities outside the payment system, causing significant losses across the economy and turning into a national security concern.

Other challenges relate to lack of standardization to validate the security of biometric data for payments, as this creates barriers to interoperability when multiple vendors or business partners need to be integrated in the production chain. Nonetheless, ongoing innovation as well as industry and government initiatives can help advance the use of biometric technologies, mitigate the risks of centralized databases and develop domestic and international standards.

Bottom line

Biometric authentication will continue to grow at a fast pace creating new business and employment opportunities, while transforming payment and non-payment transactions. Rapid adoption is allowing banks to boost security, enhance the customer experience and improve efficiency. New developments will provide additional benefits such as creating a fully integrated multichannel environment and across industries in a seamless fashion.

Digital news

OECD releases its Digital Economy Outlook 2015

The report covers the current status and outlook of the digital economy, the main trends in the ICT sector, an overview of ICT demand and adoption, the developments in communication policy and regulation and the effects of the digital economy on growth and development. Besides, special chapters are dedicated to developments in security and privacy and to the emerging 'Internet of Things'.

Bank of Spain reports on payment systems oversight in 2014

The annual report shows the evolution and most relevant changes in the Spanish payment systems during 2014, as well as the oversight activities carried out by the central bank. Despite the decrease in the number of cards in circulation with respect to 2013, card-based payments gained market share in 2014 as their value grew up by 7.43%, more than the increase in private consumption.

First draft standard on ISO 20022 for real-time payments published

The ISO Real-Time Payments Group (RTPG) has published a first draft of ISO 20022 messages to be used by the global payments industry. This first draft is focused on helping countries with their domestic implementation, and also with ensuring interoperability between systems. The initial specification is currently being circulated for review and comment ahead of a further meeting at the international Swift banking conference (Sibos) which is being held in October.

US Treasury seeks public comments on marketplace lenders

The U.S. Treasury Department has launched a Request for Information (RFI) published in the Federal Register available until September 30, 2015. The information requested will allow policymakers the study of various business models and products offered by online marketplace lenders, the potential for online marketplace lending to expand access to credit to historically underserved borrowers, and how the financial regulatory framework should evolve to support the safe growth of this industry.

FED appoints Faster Payments strategy leader

The Federal Reserve System announced the appointment of Federal Reserve Bank of Chicago Senior Vice-President Sean Rodriguez as its Faster Payments Strategy Leader.

FCA about the Payment Systems Regulator (PSR)

The UK Financial Conduct Authority released a paper explaining the proposed method for calculating and collecting PSR's fees from participants in regulated payment systems.

DISCLAIMER

This document, prepared by BBVA Research Department, is provided for information purposes only and expresses data, opinions or estimates pertinent on the date of issue of the report, prepared by BBVA or obtained from or based on sources we consider to be reliable, which have not been independently verified by BBVA. Therefore, BBVA offers no warranty, either express or implicit, regarding its accuracy, integrity or correctness.

Estimates this document may contain have been undertaken according to generally accepted methodologies and should be considered as forecasts or projections. Results obtained in the past, either positive or negative, are no guarantee of future performance.

This document and its contents are subject to changes without prior notice depending on variables such as the economic context or market fluctuations. BBVA is not responsible for updating these contents or for giving notice of such changes.

BBVA accepts no liability for any loss, direct or indirect, that may result from the use of this document or its contents.

This document and its contents do not constitute an offer, invitation or solicitation to purchase, divest or enter into any interest in financial assets or instruments. Neither shall this document nor its contents form the basis of any contract, commitment or decision of any kind.

With particular regard to investment in financial assets having a relation with the economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions on the information contained in this document. Persons or entities offering investment products to these potential investors are legally required to provide the information needed for them to take an appropriate investment decision.

This report has been produced by the Financial Inclusion Unit:

Chief Economist
David Tuesta
david.tuesta@bbva.com

Javier Alonso
javier.alonso.meseguer@bbva.com

Noelia Cámara
noelia.camara@bbva.com

Pablo Urbiola
pablo.urbiola@bbva.com

Isabel Vegas
isabel.vegas@bbva.com

With the contribution of:

Alfonso Arellano Espinar
alfonso.arellano.espinar.contractor@bbva.com

US
Nathaniel Karp
Nathaniel.Karp@bbva.com

BBVA Research

Group Chief Economist
Jorge Sicilia Serrano

Developed Economies Area
Rafael Doménech
r.domenech@bbva.com

Spain
Miguel Cardoso
miguel.cardoso@bbva.com

Europe
Miguel Jiménez
mjimenezg@bbva.com

US
Nathaniel Karp
Nathaniel.Karp@bbva.com

Emerging Markets Area

Cross-Country Emerging Markets Analysis
Alvaro Ortiz
alvaro.ortiz@bbva.com

Asia
Le Xia
le.xia@bbva.com

Mexico
Carlos Serrano
carlos.serranoh@bbva.com

LATAM Coordination
Juan Manuel Ruiz
juan.ruiz@bbva.com

Argentina
Gloria Sorensen
gsorensen@bbva.com

Chile
Jorge Selaive
jselaive@bbva.com

Colombia
Juana Téllez
juana.tellez@bbva.com

Peru
Hugo Perea
hperea@bbva.com

Venezuela
Oswaldo López
oswaldo.lopez@bbva.com

Financial Systems and Regulation Area
Santiago Fernández de Lis
sfernandezdelis@bbva.com

Financial Systems
Ana Rubio
arubiog@bbva.com

Financial Inclusion
David Tuesta
david.tuesta@bbva.com

Regulation and Public Policy
María Abascal
maria.abascal@bbva.com

Recovery and Resolution Strategy
José Carlos Pardo
josecarlos.pardo@bbva.com

Global Coordination
Matías Viola
matias.viola@bbva.com

Global Areas

Economic Scenarios
Julián Cubero
juan.cubero@bbva.com

Financial Scenarios
Sonsoles Castillo
s.castillo@bbva.com

Innovation & Processes
Oscar de las Peñas
oscar.delaspenas@bbva.com

Contact details:

BBVA Research
Azul Street, 4
La Vela Building - 4 and 5 floor
28050 Madrid (Spain)
Tel.: +34 91 374 60 00 and +34 91 537 70 00
Fax: +34 91 374 30 25
bbvaresearch@bbva.com
www.bbvaresearch.com