BBVA | RESEARCH

Digital Economy Outlook

JUNE 2016 | DIGITAL REGULATION UNIT

Index

Summary

Who are the RegTechs? Characterisation of FinTech companies focused on regulatory issues

RegTech companies have emerged as a bridge between businesses and their regulatory compliance supervisors. Those start-ups differ from the existent players in the use of technologies like cloud computing, big data or the blockchain. However, incumbents in the field are starting to react by adopting new technologies or by acquiring promising companies.

eIDAS: New framework for electronic identification and e-signatures in Europe

The eIDAS Regulation aims to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. It consists of two basic sections, the first relating to cross-border electronic identification and the second to trust services (which include electronic signatures).

Open data: big data to better serve the citizens

Access and reutilization of data to develop new services are two of the foundations of the digital economy. Governments and public authorities are now promoting open access to data, since they are well aware of their potential for boosting economic growth.

1 Who are the RegTechs?

Characterisation of FinTech companies focused on regulatory issues

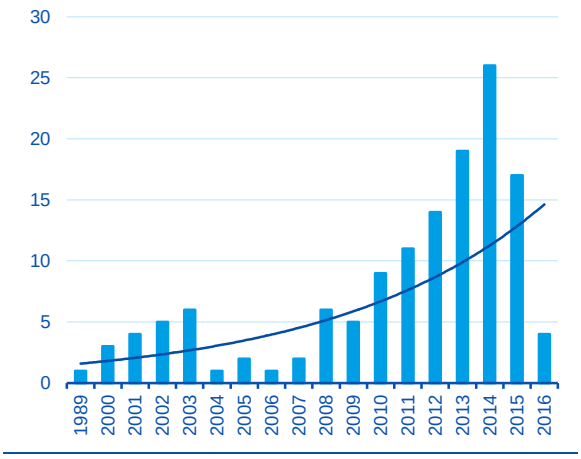
RegTech companies have emerged as a bridge between businesses and their regulatory compliance supervisors. Those start-ups differ from the existent players in the use of technologies like cloud computing, big data or the blockchain. However, incumbents in the field are starting to react by adopting new technologies or by acquiring promising companies.

In a recent paper published by BBVA Research[1], we defined RegTech as a set of companies and solutions that marry innovative technology and regulation to meet regulatory requirements across industries, including financial services. But who are these companies? In this article we will focus on the number of emerging RegTechs, their location and the regulatory areas in which they are working.

Start-up landscapes

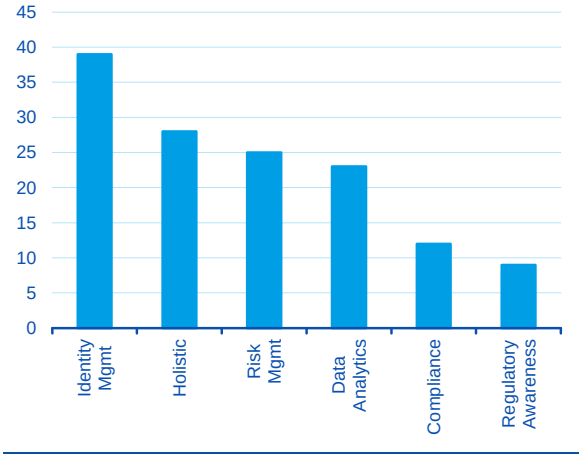
Although the term RegTech has only recently been coined, **in the last years a growing number of start-ups have developed solutions to satisfy regulatory compliance needs**. The following image displays the increasing pace of birth of RegTech companies, and is the result of an analysis of 135 start-ups.

Figure 1.1
Number of RegTech companies founded per year 2000-2016 (as of April 2016)



Source: BBVA Research

Figure 1.2
Number of RegTech start-ups per regulatory areas



Source: BBVA Research and Haver

Although those companies have a common regulatory focus, we have found differences in their area of expertise. In a recently published report, the IIF identified seven main regulatory areas where RegTech solutions can fit[2]. However, when analysing companies, we have found difficulties in classifying some into these categories, due to a lack of information or to the fact that some companies work on areas not specifically identified by the IIF. In order to simplify our classification, we are using five broader categories:

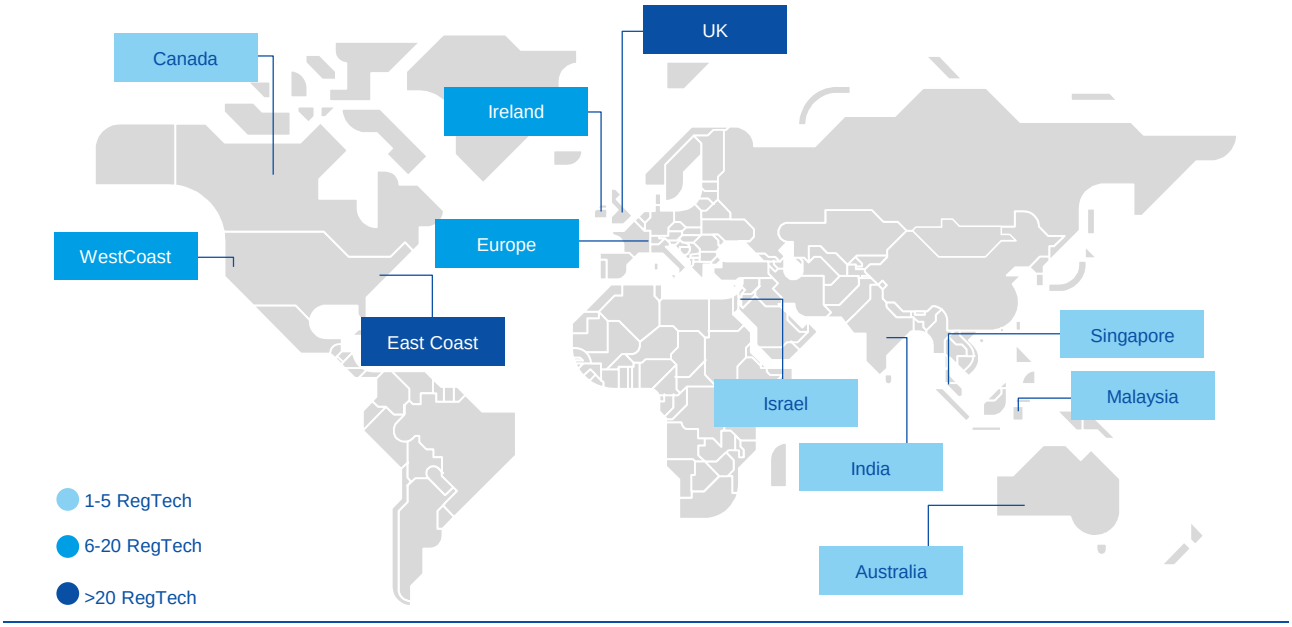
- **Identity Management**: Includes companies that focus on KYC/AML/CFT regulations, associated to customer identity management and anti-fraud processes. This is the most common type in our study.
- **Risk Management**: Includes companies capable of automatically identifying and managing sources of risk through pattern analysis and information management.

1: Casadas, V. and Sebastián. J. (2016) *RegTech, the new magic word in FinTech.* Digital Economy Outlook (pp. 4-5). BBVA Research.
2: van Liebergen, B. et al. (2016) *Regtech in Financial Services: Technology Solutions for Compliance and Reporting.* IIF publications.

- **Analytics & Reporting**: Includes companies that use advanced technologies for the storage and analysis of large volumes of structured and unstructured data, usually for reporting purposes.
- **Compliance**: Includes companies that automatically monitor compliance with the company's policies and procedures, laws and regulations, from customer protection processes to tax issues and trading. Due to the high amount of companies specialising in ID issues and the potential use of alternative technologies, like biometrics, ID management is included in another category.
- **Regulatory awareness**: Includes companies that automatically identify and interpret regulatory changes and allocate the different compliance obligations. This is the least common type.

Some of these categories may slightly overlap, and of course there are companies that provide solutions in more than one category. In this last case, we include the company in a sixth category that we have called "**Holistic**", which is the second-most common category.

Figure 1.3
Number of RegTech start-ups by geographies



Source: BBVA Research

Finally, we need to mention **the importance of new technologies in this environment**. This is not an exhaustive review but, to mention just a few: cloud computing can be considered a basic requirement for most RegTechs, big data techniques are essential to process large quantities of structured and unstructured information, blockchain is used to deliver real-time transparent tamper-proof information while artificial intelligence is of great use in analysing regulatory changes.

The incumbents landscape

Several companies have already been providing solutions to address regulatory requirements for several years before this sudden "explosion" of new RegTech start-ups. Governance, Risk and Compliance (GRC) software platforms, Enterprise Risk Management (ERM) tools and consultancies providing personalised advice are examples of this. Now, the incumbents in this space are seeing how the newcomers are trying to cannibalise their business, and in some cases are already reacting by following different strategies. The opportunities lie in developing new digital skills in-house, improving portfolio products with technologies like cloud-based platforms, or obtaining that expertise by acquiring RegTech companies. **In the near future, incumbents that are not able to capture the value of digital technologies and streamline their**

processes to deliver agile regulatory compliance solutions will probably be set aside by these new entrants.

Future scenarios

RegTech is still an immature market hence it is hard to predict how the RegTech ecosystem will evolve. However, we envisage three potential future scenarios as being most probable:

- In the first scenario, **incumbents in the GRC space adapt their offer** to the new needs of banks by adopting these new technologies. The adoption may vary among incumbents, from internal development to partnerships with RegTech start-ups, or even acquisitions.
- In the second scenario, **one or more RegTech start-ups grow enough to become leaders** in their regulatory area, competing face-to-face with current incumbents or even displacing some of them.
- In the third scenario, **several RegTech start-ups partner with the aim to offer a holistic solution** for all regulatory needs, creating a super-company to grab market share from incumbents.

It is too soon to know how these scenarios will develop but, based on lessons learned from other innovative ecosystems, a mix of the three is more likely to become the final picture.

2 eIDAS: New framework for electronic identification and e-signatures in Europe

The eIDAS Regulation aims to provide a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. It consists of two basic sections, the first relating to cross-border electronic identification and the second to trust services (which include electronic signatures).

Context and background

The creation of a climate of trust is essential for the development of the digital economy. Distrust, due in particular to perceived legal uncertainty, makes consumers, businesses and public authorities hesitate to carry out transactions electronically or adopt new services.

In 2010 a report by the European Commission entitled "A Digital Agenda for Europe" indicated that the fragmentation of the digital market, the lack of interoperability and the increase in cybercrime constituted significant obstacles to the take-off of the digital economy. In another report on citizenship in 2010, entitled "Dismantling the obstacles to EU citizens' rights", the Commission highlighted the need to resolve the main problems preventing EU citizens from enjoying the benefits of a digital single market and cross-border digital services. In 2011 the European Council asked the Commission to create a digital single market in order to progress rapidly in key areas of the digital economy and to promote a fully integrated digital single market, facilitating the cross-border use of online services, with particular attention to secure electronic identification and authentication.

In this context, the eIDAS Regulation, published in 2014, aims to harmonise Member States' electronic identification systems and achieve mutual recognition for services provided online by public bodies in terms of cross-border authentication. One of the regulation's aims is to strengthen trust in electronic transactions within the European internal market. In this way it provides a common foundation to enable secure electronic interactions among citizens, businesses and public authorities, and increases the effectiveness of public and private online services, digital business and e-commerce in the EU.

The regulation consists of two main sections. The first is dedicated to **cross-border recognition of Member States' national electronic identification schemes** for accessing the electronic services of other Member States' public authorities. The second outlines a **single legal framework applicable throughout the EU for providers of trust services such as electronic signatures**, electronic seals, electronic time stamps, certified electronic delivery services and website authentication certificates.

What does all this mean for citizens and businesses?

In the near future citizens and businesses should be able to use their electronic identifiers (eID) issued by one Member State to access any online service of another Member State. For example, a British citizen could consult the research projects put out to tender by the Spanish public authorities and apply for the relevant scholarships or grants using his UK-validated eID as the means of identification.

This mutual recognition of Member States electronic identification schemes must be up and running by September 2018.

Nearly all Member States already have eID solutions to a greater or lesser extent. Among the government initiatives for establishing electronic identification systems, we can mention GOV.UK Verify in the UK, with a federated system that uses a number of different providers, Cl@ve in Spain, as an example of a centralised

system, and cross-border interoperability pilot schemes such as STORK, using a system shared among countries. The latter has served as the basis for the technical implementation of eIDAS.

If these cross-border electronic identity verification mechanisms of the Member States are opened up to the private sector, the opportunities for developing a pan-European digital market multiply.

In the case of banking, having an electronic identification system in which the real identity is verified represents a great advance and facilitates, in particular, the process of starting a business relationship with new customers through digital channels. In the financial sector there are certain restrictions on initiating business relations remotely, normally associated with the regulations on the prevention of money laundering and the financing of terrorism, and in particular with banks' obligation to identify the customer in a reliable manner before contracting any product or carrying out certain transactions. In general, all these due diligence mechanisms make the user experience of signing up as a customer of a financial institution through digital channels relatively slow and difficult compared with the standards set by the Internet giants, which most customers consider as a benchmark. The use of eID systems incorporating persons' validated real identity would be hugely helpful in the identification phase of the new customer sign-up process. It would simultaneously allow compliance with the assurances demanded by the law and offer customers a simpler and more convenient user experience.

As well as Member States' national eID schemes, there are also electronic identification initiatives in the private sector, such as GSMA Mobile Connect, led by telecommunications operators, and environments headed up by the financial sector such as Tupas (Finland), NemID (Denmark) and BankID (Norway), in some cases in collaboration with the corresponding governments.

As for the *trust service providers*, eIDAS also introduces some new features. It establishes mechanisms whereby services delivered by providers that have been certified and appear in the *Trusted Lists* (EUTL) in any Member State will be valid and recognised throughout the EU. Furthermore, electronic signatures for legal persons (companies and organisations) are eliminated and will now be associated only with natural persons (private individuals). The concept of electronic seal is introduced as the mechanism for certifying the source and integrity of documents originating from legal persons, bearing in mind that an electronic seal is not the electronic signature of the legal person.

The new features of eIDAS relating to trust services and electronic signatures will be applicable with effect from 1 July 2016.

The new eIDAS Regulation is another step towards the Digital Single Market. It establishes the legal framework for digital identities and e-signatures to have cross-border validity. In any case, eID and electronic signature systems must offer not only security, but also a good user experience, in order to popularise their use so both the public and the private sector can take advantage of their potential. In short, electronic identity and signatures should help to facilitate electronic interactions and transactions, and to boost the European economy.

3 Open data

Big data to better serve the citizens

Access and reutilization of data to develop new services are two of the foundations of the digital economy. Governments and public authorities are now promoting open access to data, since they are well aware of their potential for boosting economic growth.

Data and open access

Ever since the prestigious magazine *The Economist* published its article entitled "The data deluge"[3] in 2010, the term *big data* has been one of the mantras of the new internet age. The exponential growth in the volume of data produced, combined with the falling processing and storage costs, allows us nowadays to have detailed information on almost any aspect of life or of our environment. Data are the basis of the internet economy, and the flow of data now generates more economic value than global goods trade[4].

In the broadest sense, open access initiatives encompass, inter alia, free software, open source software, open access to scientific knowledge, as well as open data. The latter seek to make the data generated by the public authorities available to society at large, so that any citizen or business can use them to generate information and knowledge or develop new services. According to the consultancy firm McKinsey, open data could help unlock US$3 trillion a year in economic value in seven sectors: education, transportation, consumer products, electricity, oil and gas, healthcare and consumer finance[5].

In order for these initiatives to be possible, data must not only be available but also accessible and re-usable, which implies the use of open standards for their publication and user licences allowing their redistribution or combination with data from other sources, as well as having an appropriate cost. Interoperability is achieved with the use of shared protocols (such as APIs), taxonomies and standardised formats and by means of creating repositories in which to make data easily available.

In developing these initiatives, it is also necessary to consider the legal constraints relating to privacy and security, as well as the legislation of each particular country, as regards to both the access and distribution of data and the possible cost derived from their use.

Government open data initiatives

Governments and public authorities are among the main collectors of data, and by their very nature must seek the best possible use of this resource for the benefit of their citizens. One way of attaining this objective is without doubt to develop policies of free access to data. There are open data initiatives at every level of the administration, and they can be driven by governments themselves, pressure groups working on a particular subject or by citizens themselves.

National statistics on education, housing, healthcare, etc., data on public budgets and spending, national maps (including postal codes), data on public transport and data from public agencies, such as the Meteorology Office, are some of the data that governments can open to allow the construction of new services by citizens, businesses or other public authorities. Data from cultural institutions such as museums, archives and libraries could also be exploited, although in this case there may be greater constraints as regards to intellectual property rights.

3: "The data deluge", *The Economist*, 25 Feb. 2010
4: Manyika, James, et al. *Digital globalization: The new era of global flows*, McKinsey Global Institute, 2016
5: Chui, Michael, et al. "What executives should know about open data", *McKinsey Quarterly*, Jan. 2014

The objectives of these open data policies and, more broadly, of **open government** policies, are to achieve greater transparency and increased citizen participation in public life, as well as to reduce costs by facilitating cooperation among different authorities thanks to the interoperability of data.

One of the pioneering public initiatives in opening up data is that of **"smart cities."** Combining data from a variety of sources (sometimes including networks of sensors) allows to generate patterns of behaviour, which helps improving services at local level, such as public transport and emergency services.

Among the countries that stand out in these kinds of policies, the **United Kingdom** heads both the annual ranking published by the Open Knowledge Foundation (an index[6] measuring access to key indicators, covering 122 countries and 1,586 databases in 2015) and the Open Data Barometer of the World Wide Web Foundation[7] (covering 92 countries and measuring the degree of readiness, implementation and effect of open data programmes). The British government has promoted open access policies through a variety of programmes such as the Public Data Group, which operated from 2011 to 2015.

As for the **European Union**, as part of its Digital Single Market strategy, the Commission published *Directive 2013/37/EU (the PSI Directive)*[8] on the re-use of public sector information. This directive seeks to harmonise the types of public data available for re-use in the internal market, in accordance with the relevant access system (amending Directive 2003/98/EC). It encourages countries to allow access to and re-use of as much information as possible, and places limits on agreements granting exclusive rights to data. Nevertheless, there continue to be differences among Member States, which may hamper developments covering more than one country, where account must be taken of the different regulations and possible payment of fees for the use of data.

A key point in the European open data ecosystem is the creation of a pan-European data portal. In December 2014 the Commission launched the project for the creation of the European Data Portal, which harvests public access metadata from all over Europe.

In the **United States** open government has been driven by the Open Government Directive of 2009, which was based on the principles of transparency, citizen participation and collaboration, and required all government agencies to include at least three significant data sets in the portal *data.gov*[9]. This portal currently contains more than 180,000 data sets.

Conclusion

There is a clear awareness on the part of the public authorities of the potential for economic development represented by the implementation of open access policies, and initiatives are being carried out to make public data easily accessible and re-usable in the development of services and the creation of value. However, much remains to be done in terms of making regulations more uniform and standardising access so as to facilitate overall developments, within the constraints of privacy and personal data protection.

6: Open Knowledge Foundation, *Global Open Data Index*
7: World Wide Web Foundation, *Open Data Barometer*
8: Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information, OJEU 27 June 2013. 2013
9: Open Government Directive, US Government, 2009

DISCLAIMER

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

Estimations 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.

In regard to investment in financial assets related to economic variables this document may cover, readers should be aware that under no circumstances should they base their investment decisions in the information contained in this document. Those 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 Digital Regulation Unit:

Chief Economist for Digital Regulation Unit
Álvaro Martín
alvaro.martin@bbva.com

Vanesa Casadas
vanesa.casadas@bbva.com

Israel Hernanz
israel.hernanz@bbva.com

Alicia Sánchez
alicia.sanchezs@bbva.com

Javier Sebastián
jsebastian@bbva.com

Pablo Urbiola
pablo.urbiola@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

Turkey
Alvaro Ortiz
alvaro.ortiz@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
Julio Pineda
juliocesar.pineda@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

Digital Regulation
Álvaro Martín
alvaro.martin@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:

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