Original My - Business Overview

Edilson Osorio Junior, Miriam Tomie Oshiro, Helena Suarez Margarido
OriginalMy.com

October 2017

1. About the Company

OriginalMy is a company originally incorporated in 2015 in Brazil by an experienced founding team, focused on developing blockchain applications.

Over the past years, it has been in the spotlight regarding blockchain solutions in Latin America. As a result, the company was selected and joined 02 highly disputed acceleration programs, Accenture Up Innovation Lab and Google Campus Sao Paulo.

After receiving a seed investment (early 2017), it has focused on creating end-to-end blockchain applications that solve old problems in the real world. Such applications are currently available online and on mobile (iOS and Android), which reinforces the team's execution capabilities and the company's ability to foresee market's needs and propose full solutions.

For the reasons presented in the whitepaper, OriginalMy has decided to conduct the first initial token offer to be held in Brazil by the end of October 2017.

Therefore, the purpose of the present paper is to present the market in which the company has been inserted, bringing relevant information and providing highlights on the current business strategy.

2. Market Overview

Identity is a common resource used / required by many services, both online and offline. However, most digital IDs rely on centralized entities (who are responsible for issuing digital identity tokens) or are based on proof of knowledge or ownership (of private key, password to access a previously provided e-mail, holding a given cell phone number, etc).

That said, every known Digital ID form is **based on assumptions**: that no document forgery has occurred, the person is the only one who has access to its phone and no hack to its e-mail has occurred. Considering such premises are all correct, such Digital IDs allow to some level of safety when sharing information or signing documents, for instance.

However, **those assumptions are not always true**. Cases of hacks or fraud are countless and may involve big service providers such as Google[1]. On the other hand, centralizing personal data with third trusted parties may lead to excess and much privacy discussion, as seen recently in the Equifax case[2].

Despite the effort that has been made in the past years, proving that one person is who he/she alleges to be in online ambience has no indisputable proof so far. Still, the need of enforceability on online actions, including contracts and payments, lead to entire industries to arise that currently consist on relevant markets.

2.1. Digital Identity

Ever since internet use was widespread, companies could count on one distributed network to reach global markets with no need of physical travel. However, because the only identification on the network is made by using IP addresses (which can easily be altered or even hidden), fraud and hacks are relevant part of everyday online businesses.

Seeking for mitigation, some governments have released their own regulations establishing rules for the issuance of online IDs that would, however, always count on third trusted parties (e.g. Brazil and France have their own rules for issuing those IDs, which require a centralized certifying authority).

Notwithstanding that the problem on IDs issuance was brought to the United Nations attention with recent cases of refugees requiring political asylum in other countries, that had no means to prove who they were and where they came from. Currently, the United Nations estimates that 1.1 Billion people live without an officially recognized identity[3].

Given that the right to be recognized "*everywhere as a person before the law*" is stated on article 6 of the Universal Declaration on Human Rights, identity is not an attribute to be given by any national state, but a human right instead. Using that approach, the United Nations aims to have some form of global identity fully implemented by 2030[4].

Probably because such approach is unorthodox, we could not locate any type of Digital ID solutions that count on something different than trusted parties or assumptions (e.g. holding a physical USB token, having access to an e-mail address, etc.) to be issued.

Nevertheless, the market of personal ID credentials was valued at $8.7 billion in 2016, with expected growth for the upcoming years[5].

2.2. Digital and Electronic Signatures

Electronic signatures are technically defined as the use of any electronic means to sign (express wiliness to) determined digital document. Its broad definition leads to many so-called electronic signatures solutions and are usually based on the assumption that each party has access to a determined electronic service and/or device (e-mails, cell phones, etc).

Digital signatures, also by technical definition, are electronic ones that count on a cryptographic layer. Despite also counting on assumptions (e.g., signees must hold the private key), it provides an extra layer of security in terms of what has been signed, that shall not be changed thereafter.

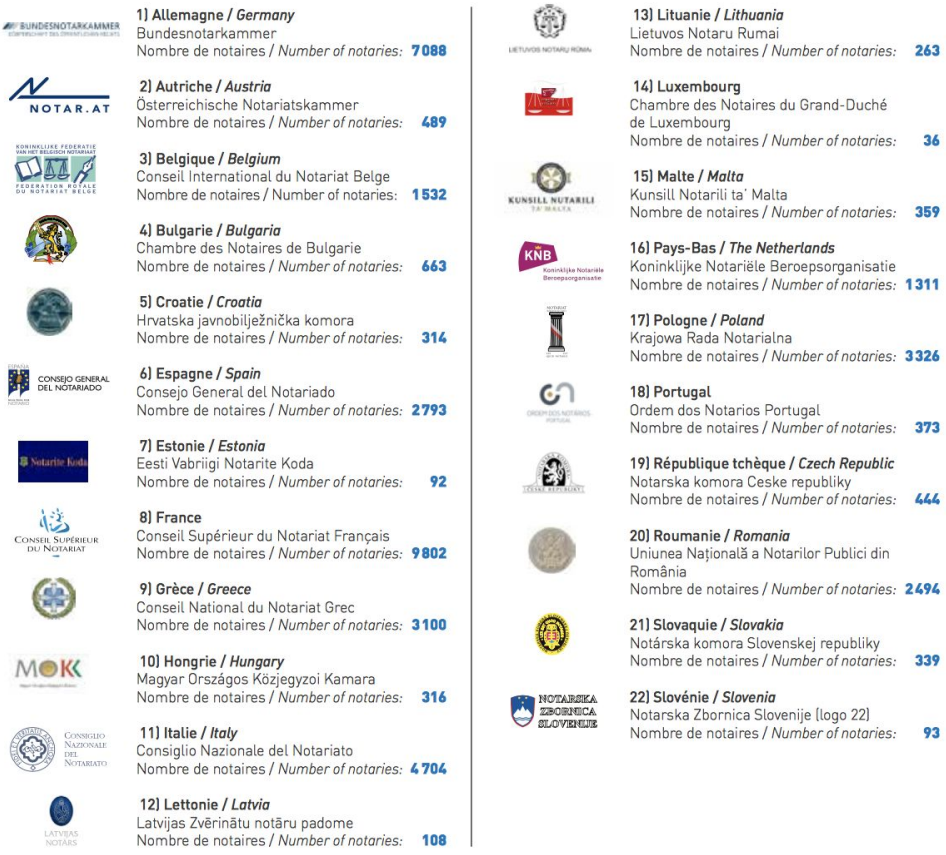
Market analysis statistics are extremely hard to access since many of them do not consider the distinction between electronic vs. digital signature markets. Nonetheless, considering the broadest concept, some studies have estimates the global e-signature market to grow at a CAGR of 34.7%, to reach approximately $9 billion by 2023[6].

2.3. Notaries & Centralized Registries

The institution of notaries is common in Civil Law countries[7], where Public Registry laws are usually into force. They usually constitute on a person or company that holds what is known as "full faith and credit", i.e., the authority delegated by a government to certify the authenticity of documents and/or information.

However, centralized registries can be found often in Common Law countries[8], as it is a rule that centralized organisms, companies and/or persons are entitled to hold information and, thus, are the only ones able to testify their authenticity[9].

According to information released by Council of the Notariats of the European Union (CNUE), in 2016 there were over 40,000 notaries[10] in the member states:



Other Civil Law countries, such as Brazil, also count on relevant notaries per person ratio. In that case, the 7.628 notaries were responsible for a gross revenue of nearly $4 billion[11] in the past 12 months.

Although there are several types of notaries in Europe[12], recent information on the Lithuanian market[13] may help to narrow the market cap for the continent: the yearly gross revenue was of $60,000 per notary in 2014 and $90,000 in 2015, approximately. That would allow a high-level estimate of the European market cap between $2,4 and $3,6 billion.

In Common Law countries, one would not see such a relevant market opportunity. However, some estimates account that alternatives to the traditional paper notarization system could enjoy a $30 billion market opportunity[14].

Because most of markets are centralized, it is considerably difficult to find public reputable data on the market size. Despite that, only by considering the highlighted markets presented herein, it is plausible to consider the market cap of being not less than $36,4 billion.

2.4. KYC and Compliance

Given the complexity of traditional financial services, in the past years the technology market has been witnessing an exponential growth of the *fintechs*, i.e., companies that are willing to approach such market with new technological solutions.

However, regulations are quite complex and require substantial effort and resources from companies that act in such a market not only to access reliable data when subscribing their customers, but also to keep such information updated.

Therefore, it should come as no surprise that recent studies indicate the growth of investments on compliance in the upcoming years[15].

Considering financial institutions only, a research conducted in 2016 showed that among 800 interviewed companies, the average costs to meet KYC and Customer Due Diligence (CDD) compliance was of $60 million[16], which represents a $48 billion market for that industry.

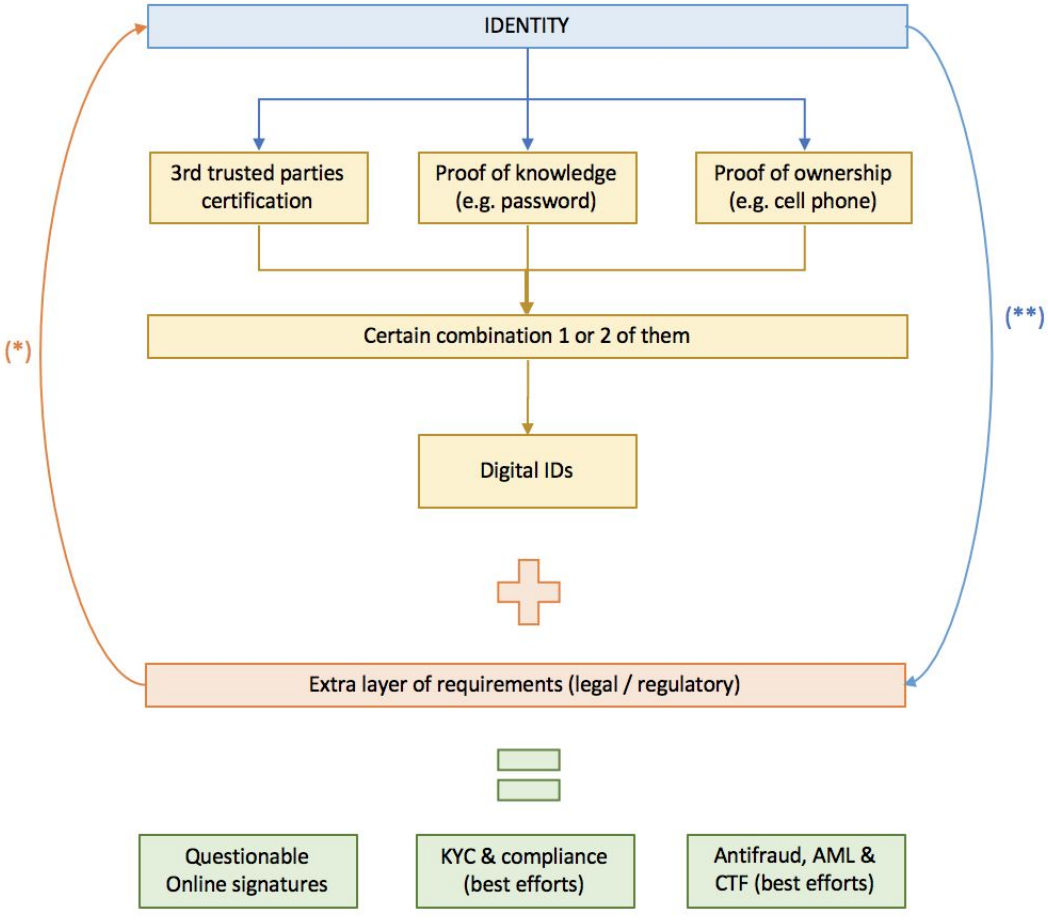
2.5. Fraud, AML & CTF: Detection and Prevention

Due to the absence of reliable data, especially when digital environments are regarded, efforts on services that act on fraud detection and prevention and Anti Money Laundering solutions have played an important role on digital services in the past years.

The market cap, estimated at $9.62 billion in 2014, is expected to grow to a $21.44 billion by 2019, at a CAGR of 17,4%[17].

2.6. Current industry scheme

As a consequence of the aforementioned, the current scenario for the industry has to consider weak forms of ID verification, especially in online ambience. Therefore, the inefficiency of this current $111 billion industry can be summed up as follows:



(*) Request for additional information / documents (multiple times)
(**) Sending additional information / documents (multiple times)

3. Market Definition

For purposes of this analysis, we have considered the relevant market to be composed by every service that count on "weak" forms of ID verification, i.e., that rely purely on third trusted parties' certifications or considers proof of ownership and/or knowledge as trusted sources for assessing identification.

Also, accepting identity as a human right approach, the geographic market has been defined as global, as the centralization on ID issuance and increasing compliance regulations are worldwide phenomena.

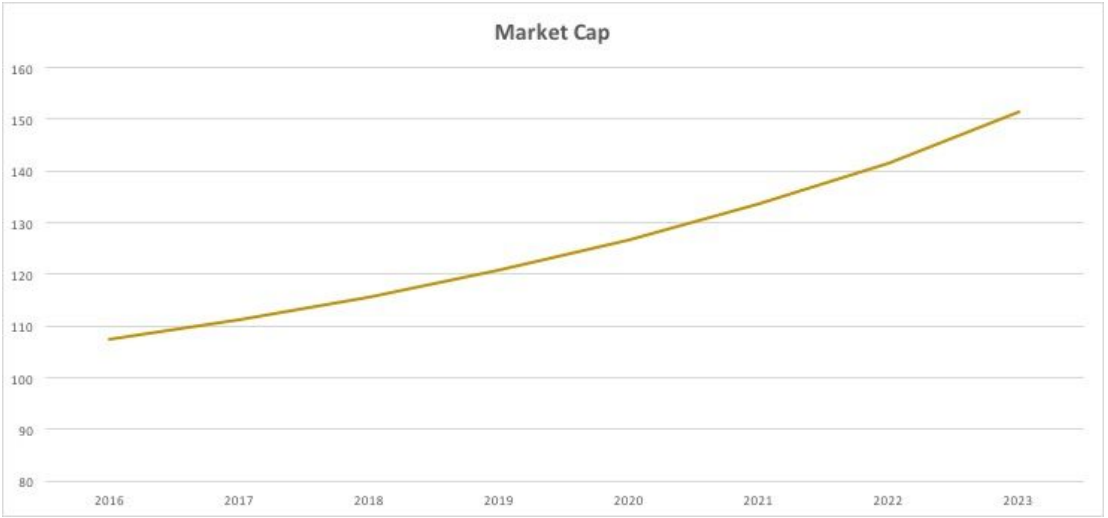
4. Business Highlights

4.1. Market Cap

The relevant market presented great historical growth in the past years. More specifically, ever since the 2008 economic crisis, regulatory enforcements have been increasing and data verification of all sorts became a growing concern due to legal impositions.

That is possibly the main reason why studies have shown great increase potential for the industry in the upcoming years.

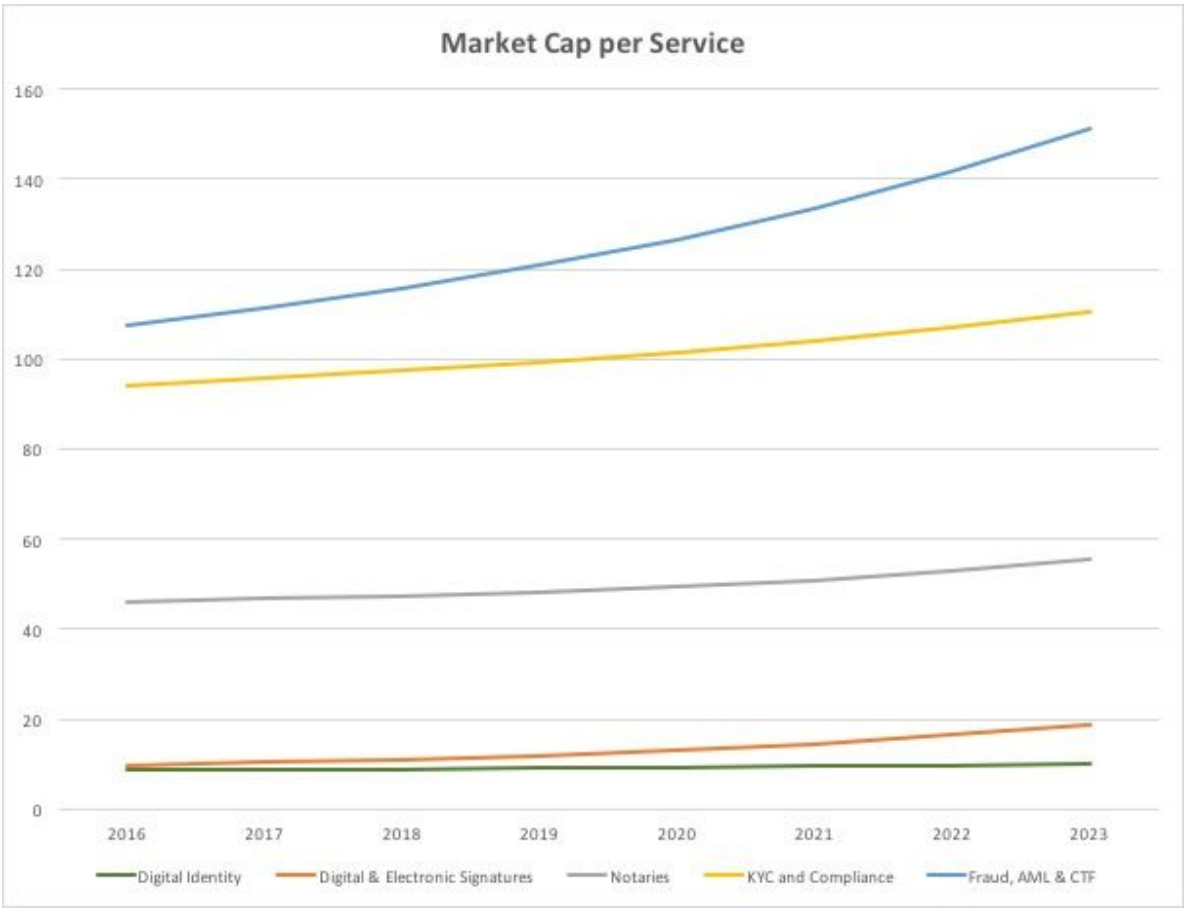
4.1(a): Overall Market Cap - History and Estimation:



Graph 1: Estimated Market Cap growth from 2016 to 2023

Even if the services that compose such market are individually considered, relevant growth is still expected.

4.1(b): Market Cap per Service - History and Estimation:



Graph 2: Estimated Market Cap per Service growth from 2016 to 2023

It worth mentioning that the lower year-over-year expected increase in on Digital Identity services. That reinforces the underestimation of such services and is the key to understand the absolute inefficiency of the current industry scheme (item 1.6).

4.2. Segmentation

Although there are many players in specific services that compose the market, there are none approaching “assumptionless” digital ID services nor services based on that. For that, even though the presented services seem highly competitive if individually considered, the market space as defined can be deemed as blue ocean.

4.3. Business Strategies

a) Vertical Integration

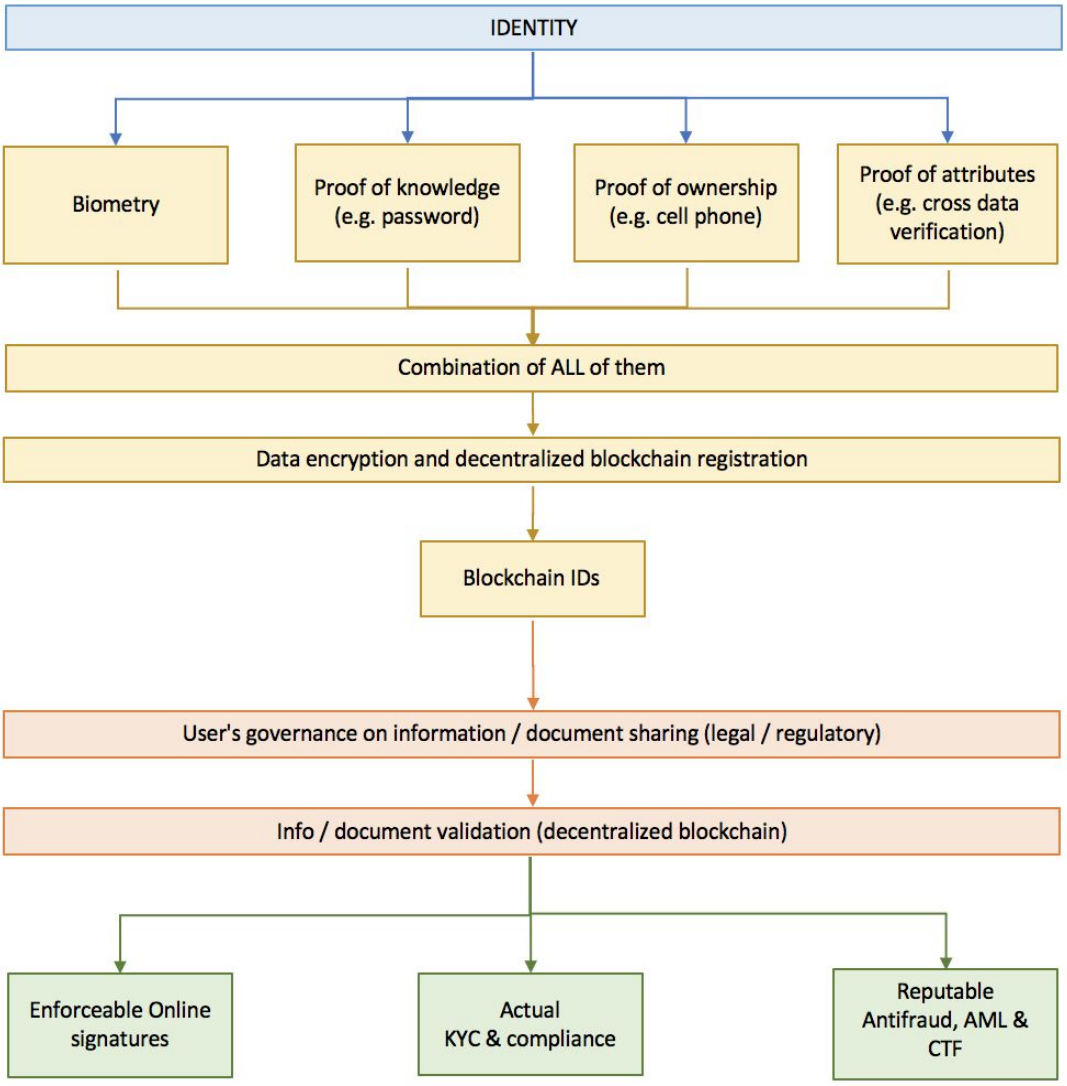
As mentioned before, the absence of a reliable digital ID form leads much effort and money being spent to fulfill regulatory requirements by multiple stakeholders.

Besides considerable amount of rework for accessing and validating information and documents, when it comes to online ambience most services provided result in “almost as good” as non-digital ones, working on best efforts basis.

OriginalMy proposes a new approach to the issue. By providing strong, decentralized and storage-free proofs of identity, the company focuses on developing applications that integrate such form of digital ID (“Blockchain ID”) to the other aforementioned services.

The current services provided by the company include digital documents registration, KYC verification and online signatures. The available applications can also be used to create reputable anti-fraud solutions, AML and CTF enforcement.

By integrating multiple service layers, the company can provide end-to-end solutions and disrupt the current industry scheme, as follows:



b) Blockchain ID decentralization

Persons and companies' data are theirs only and all should be entitled to prove themselves as a person before the law. That said, their IDs are no one's to hold, nor to control its issuance.

Even though OriginalMy has developed what is probably one of the only ways to prove a person's identity in digital environments, the best incentive that one could have to keep updated accurate verifiable data is by creating a decentralized network of which it is a party.

Despite current Blockchain IDs rely on public decentralized blockchains and are issued at no cost by OriginalMy, ideally one should be able to issue it without needing a third trusted party.

For that, as part of our business strategy we intend to create a new protocol that counts on its own mining, blockchain and incentives, as a way of empowering people and granting their inherent right as human beings of holding an ID regardless of any national state.

By designing a decentralized ID network, we estimate the adoption will increase exponentially. Therefore, even though providing an open-source protocol for other companies to create applications on top of, OriginalMy will be able to count on decentralized network effect for gaining traction on the applications that will run on such network from day 01.

5. References

[1] https://www.forbes.com/sites/thomasbrewster/2017/09/18/ss7-google-coinbase-bitcoin-hack/#48ddea5b41a4 (access in September 22nd, 2017)
[2] https://www.equifaxsecurity2017.com (access in October 7th, 2017)
[3] http://id2020.org (access on October 7th, 2017)
[4] http://id2020.org/digital-identity-1/ (access on October 7th, 2017)
[5] https://www.secureidnews.com/news-item/report-personal-identity-market-worth-9-7b-by-2021/ (access on October 7th, 2017)
[6] https://www.psmarketresearch.com/market-analysis/e-signature-market (access on October 7th, 2017)
[7] http://ec.europa.eu/competition/sectors/professional_services/conferences/20051121/mateus.pdf (access on October 7th, 2017)
[8] http://www.notaryinstitute.ie/European-Union-and-the-Notary.pdf (access on October 7th, 2017)
[9] https://www.thenotariessociety.org.uk/uploads/optimadmin/document/document/69/Leaflet_-_Guide_for_Law_Graduates.pdf (access on October 7th, 2017)
[10] http://www.notaries-of-europe.eu/files/publications/cnue-annual%20report-2016.pdf (access on October 7th, 2017)
[11] http://www.cnj.jus.br/corregedoria/justica_aberta/? (access on October 7th, 2017)
[12] http://ec.europa.eu/competition/sectors/professional_services/studies/csm_standalone_en.pdf (access on October 7th, 2017)
[13] http://www.notarius.lt/publikacijos/notaries-arithmetic-260-officials-20-million-euros-of-income/?lang=en (access on October 7th, 2017)

[14]
https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=324688788 (access on October 7th, 2017)
[15]
https://www.accenture.com/t20170405T131043Z__w__/us-en/_acnmedia/PDF-47/Accenture-Compliance-Risk-Study-2017-Dare-To-Be-Different.pdf#zoom=50 (access on October 7th, 2017)
[16]
https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html (access on October 7th, 2017)
[17]
http://www.prnewswire.com/news-releases/global-fraud-detection-and-prevention-and-anti-money-laundering-market-2015-2019---market-will-be-valued-at-2144-billion-by-2019-from-962-billion-in-2014-300116928.html (access on October 7th, 2017)