

MARKETING PLAN:
FraudProof, A SaaS Anti-Fraud Solution
For The Digital Advertising Industry

Patrícia Raquel dos Santos Cadete

Project submitted as partial requirement for the conferral of
Master in Business Administration

Supervisor:

Prof. Luís Carlos da Silva Martins, Prof. ISCTE Business School,
Department of Marketing, Operations and General Management

October 2018

- Spine-

Acknowledgements

This thesis marks a profound career and life change for me. Two years ago, I was still a Journalist, working full-time for the Portuguese national television channel, and a newly Business Administration student.

As I write these words, I am one step closer to finishing this master's degree, while working as an International Account Manager for a mobile ad tech company. The chance to learn a new area from scratch brought new challenges and opportunities that I am immensely thankful for.

Throughout this journey, I collected knowledge and experiences that surpassed all expectations, contributing to my personal and professional development. A journey that would not be possible without the support of several colleagues, professionals and academics.

To Professor Luís Martins, for his availability, guidance and encouraging words through the elaboration of this project.

To Mobrand, for all the trust, help and insights without which the path would certainly have been more difficult. I end this chapter with a comprehensive approach to the digital advertising industry thanks to you.

To all my friends and family for putting up with my lack of availability during this time. To my best friend, António Pedro dos Santos, for supporting my dreams and decisions.

A deep and special thanks to my mother, father and brother for the endless patience, serenity, motivation and support.

Glossary

Ad exchange – automated technologic platform that facilitates the buying and selling of media advertising inventory from multiple ad networks via real-time bidding auctions.

Ad network – companies that connect supply (publishes) and demand (advertisers) as mediators.

Advertiser – company that is looking for traffic for their ads/campaigns. It can be an app or a brand that wants to promote its message/services.

API (Application Programming Interface) – program that allows communication between different machines and transference of valuable information. In mobile advertising, APIs allow developers to add new features to their apps easily.

Bots – bots are a type of mobile fraud.

CAC (Customer Acquisition Cost) – CAC can be calculated by dividing the marketing expenses on acquiring customers by the number of customers acquired in the same period.

Campaign – ads that share the same advertising target.

Chargeback – when the advertiser refuses to pay what was negotiated. Normally, chargebacks happened due to fraud, KPI or overspend.

Churn Rate – % of users that leave an app or game, becoming inactive users.

CPA (Cost Per Action) – the cost is associated with the action, which means the advertiser will only pay the publishers when the user completes a determined action.

CPC (Cost Per Click) – the cost is associated with a click, which means the advertiser will only pay the publisher when the user clicks on the ad.

CPI (Cost Per Install) – cost associated with an install, which means the advertiser will only pay when the user installs the app promoted by the campaign.

CPL (Cost Per Lead) – cost is associated with the lead, which means the advertiser will pay a pre-defined price for each lead generated.

CPM (Cost Per Mille) – the cost is associated with impressions, which means the advertiser will only pay the publisher then the ad was seen 1000 times.

CTR (Click-Through Rate) – number of clicks on the ad divided by number of impressions of the ad during a certain period.

CVR (Conversion Rate) – probability of user conversion after showing the ad. In the CPI industry, it is the ratio between the installs and the numbers of clicks a campaign received on a specific period.

DSP (Demand Side Platform) – allows the advertiser to buy space with the help of automation, by connecting multiple ad-exchanges and making complex media buying to determine how much to pay for a single impression.

eCPM (Effective Cost Per Mille) – revenue generated for every 1000 ad impressions, regardless of the buying method.

FAQ – frequently asked questions.

GAID (Google Advertising ID) – it is the individual identifier used by Google to identify and track unique android user devices.

Identifier/ Package Name/ Bundle ID – it identifies uniquely an application either in Apple's App Store or Google Play Store.

IDFA (Identifier For Advertising) – it is the individual identifier used by Apple to identify and track unique iOS user devices.

KPI (Key Performance Indicators) – a measurement of advertising performance. Advertisers use KPIs to evaluate traffic quality and analyse the performance of the campaigns.

LTV (Lifetime value) – in mobile advertising, LTV provides an estimate on how much revenue a particular user is likely to generate when using an app. Its purpose is to help set marketing budgets and ensure that companies use them to pursue the most effective users, maximizing effectiveness of the advertising spending.

Postback – is a proof of conversion. Attribution providers notify ad networks in real time about an app install through postback data.

Publisher – company that has traffic that wants to monetise. In other words, they sell space on their inventory so that advertisers can run advertising in their apps or mobile websites.

Rebrokering – process by which a publisher does not generate the install by themselves but, instead, rebroke the campaign to another publisher, keeping only a share in the process.

Retargeting – practice of serving ads based on previous engagement.

ROI (Return on Investment) – amount of profit gained from advertising relative to the advertising cost.

RR (Retention Rate) – percentage of users still using an app a certain number of days after the install.

RTB (Real-Time Bidding) – a subcategory of programmatic buying. Is the practice of buying and selling ads in real time instant auction.

SaaS (Software as a Service) – software delivery method which allows users to access it remotely over the internet.

SDK (Software Development Kit) – in mobile advertising, a SDK is a plugin that mobile app developers add to their app to integrate or connect to another service.

SEM (Search Engine Marketing) – marketing process that aims to increase visibility of a website in search engines through paid traffic, like Google AdWords, or by SEO.

SEO (Search Engine Optimisation) – process of optimising the visibility of a website in order to receive more organic traffic from search engine results.

SERP – search engine results page

SSP – platform that helps publishers to sell display, video and mobile ads, by mediating the demand. It allows them to connect their inventory to multiple networks, creating internal competition that, by its turn, will produce offers with higher eCPM.

Tracker – company responsible for mobile attribution. Advertisers must have a tracker incorporated into a campaign in order to have performance data, such as the number of impressions, clicks a campaign had and, furthermore, providing information about the users who converted.

Index

<i>Acknowledgements</i>	<i>III</i>
<i>Glossary</i>	<i>IV</i>
<i>Table Index</i>	<i>X</i>
<i>Figure Index</i>	<i>X</i>
<i>Annexes Index</i>	<i>XI</i>
<i>1. Sumário</i>	<i>XIII</i>
<i>2. Abstract</i>	<i>XIV</i>
<i>3. Executive Summary</i>	<i>XV</i>
<i>4. Literature review</i>	<i>I</i>
4.1. E-commerce	1
4.1.1. Software-as-a-Service	2
4.2. Digital Advertising	4
4.2.1. Mobile Advertising	6
4.2.1.1. Mobile Advertising Ecosystem	7
4.2.2. Revenue Models	10
4.3. Digital Fraud	11
<i>5. Conceptual Reference Framework</i>	<i>15</i>
<i>6. Data collection and methodology</i>	<i>18</i>
<i>7. External Analysis</i>	<i>19</i>
7.1. PESTEL Analysis	19
7.1.1. Political - Legal	19
7.1.2. Economic	20
7.1.3. Social	21
7.1.4. Technological	23
7.1.5. Environment	25
<i>8. Competitive Analysis</i>	<i>26</i>
8.1. Five Forces of Porter Analysis	26

8.1.1. Industry Rivalry _____	26
8.1.2. Threat of New Entrants _____	27
8.1.3. Bargaining Power of Suppliers _____	28
8.1.4. Bargaining Power of Buyers _____	29
8.1.5. Threat of Substitutes _____	29
8.2. Competition Analysis _____	31
8.2.1. Strategic Groups Analysis _____	31
8.2.2. Industry Life Cycle _____	33
8.2.3. Direct Competition _____	33
9. Internal Analysis _____	38
9.1. Brief contextualization of company _____	38
9.2. Mobrand's Mission, Vision and Values _____	38
9.3. Mobrand's Portfolio Analysis _____	39
10. Competitive Analysis (Internal and External) _____	41
10.1. Ansoff Matrix _____	41
10.2. SWOT Analysis _____	41
11. Survey Analysis _____	46
11.1. Questions related with key industry challenges and mobile ad fraud _____	47
11.2. Questions related with internal decisions regarding mobile ad fraud _____	47
11.3. Questions related with the launching of a SaaS anti-fraud solution _____	48
12. Project SMART Objectives _____	50
13. Development Strategy _____	51
13.1. Strategic Approach _____	51
13.2. Segmentation _____	51
13.3. Target _____	52
13.4. Positioning _____	52
13.4.1. Golden Triangle of positioning _____	53
13.4.2. Perceptual map _____	54

<i>14. Critical Success Factors</i>	<i>56</i>
<i>15. Implementation Policy Definition</i>	<i>57</i>
15.1. Marketing-Mix	57
15.1.1. Product	57
15.1.2. Price	63
15.1.3. Placement	64
15.1.4. Promotion	65
15.1.5. People	70
15.2. Technical Aspects	73
15.2.1. Technology	73
<i>16. Fundamentals for Implementation</i>	<i>75</i>
<i>17. Operational Analysis</i>	<i>77</i>
17.1. Expenses	77
17.2. Investment	77
17.3. Sales Forecast	78
17.4. Evaluation	80
<i>18. Project Conclusions</i>	<i>81</i>
<i>19. Project Limitations</i>	<i>84</i>
<i>20. References</i>	<i>85</i>
<i>21. Annexes</i>	<i>95</i>

Table Index

Table 1 – Conceptual Framework of Reference	15
Table 2 – Market Research Data	18
Table 3 – Level of the forces in the industry	30
Table 4 – Major anti-fraud players (Group 1)	34
Table 5 – Mobrand Vision, Mission and Values	39
Table 6 – Hierarchical SWOT: Internal Analysis	45
Table 7 – Hierarchical SWOT: External Analysis	45
Table 8 – FraudProof Objectives	50
Table 9 - FraudProof segmentation criteria	52
Table 10 - Detailed FraudProof segmentation criteria	53
Table 11 – Technological architecture of FraudProof	59
Table 12 - FraudProof packages	62
Table 13 – FraudProof pricing packages	63
Table 14 – Inbound Marketing Strategy	69
Table 15 – Expenses with People	72
Table 16 - Technological Expenses	74
Table 17 - Project Implementation chronogram	75
Table 18 - Expenses Map	77
Table 19 - Investment Map	78
Table 20 – Market dimension according to mobile trackers	78
Table 21 – Potential Market-target size of FraudProof	79
Table 22 – Growth Rates	79
Table 23 - Sales prediction map (in US \$)	80
Table 24 – Four year projection	80

Figure Index

Figure 1 – Flow between ad players	8
Figure 2 – Advertising Ecosystem Scheme	9
Figure 3 – Synthesis figure of Literature Review	17
Figure 4 – Industry Attractiveness: 5 Forces of Porter	30
Figure 5 – Strategic Group Analysis	31
Figure 6 – Ansoff Matrix	41

Figure 7 – Push and Pull Strategy	66
---	----

Annexes Index

Annex I – Search advertising example	95
Annex II – Display advertising example	95
Annex III – Total global spending by category (US \$ millions), at average 2014 exchange rates.....	96
Annex IV – Google's ad revenue between 2001 and 2017	96
Annex V – Smartphone subscriptions per region between 2014 and 2020	97
Annex VI – Percent of U.S Digital ad impressions by viewability and non-viewability	97
Annex VII – Attractiveness of hacking based on effort and profit	98
Annex VIII – GDP growth in the EU-28 during 2006 and 2016	98
Annex IX – GDP evolution between 1996 and 2017	99
Annex X – Unemployment rate in member states of the European Union in June 2018 (seasonally adjusted).....	99
Annex XI – EU-28 Construction, annual rate of change 2005-2017	100
Annex XII – Total attribution of Travel and Tourism to Portugal GDP	101
Annex XIII – Portuguese GVA distribution in 2016.....	101
Annex XIV – Employment distribution.....	102
Annex XV – Portugal Age Pyramids 2011, 2016 and 2080 (projection).....	102
Annex XVI – EU-28 age pyramids, 2016 and 2080 (% of total population).....	103
Annex XVII – Internet Access of households between 2012 and 2017 (% of all households)	103
Annex XVIII – Internet access in households by degree of urbanisation, 2017.....	104
Annex XIX – Subscribers of the mobile service per thousand inhabitants in 2016.....	104
Annex XX – Proportion of households with broadband internet at home - Portugal and EU28, 2010-2017	105
Annex XXI – Proportion of people with 16 and 74 years old using e-commerce in Portugal and EU, 2010-2017.....	105
Annex XXII – 5 Forces of Porter	106
Annex XXIII – FraudProof Industry Life Cycle.....	108
Annex XXIV – White Ops FraudSensor Summary Dashboard.....	108
Annex XXV – White Ops FraudSensor Explore Dashboard.....	109

Annex XXVI – White Ops FraudSensor Reports Dashboard	109
Annex XXVII – Fraudlogix Affiliate Solution Dashboard – Fraud Report	110
Annex XXVIII – Fraudlogix Affiliate Solution Dashboard – Analysis Reports	110
Annex XXIX – ForensIQ Ad Verification Solution Dashboard	111
Annex XXX – FraudScore Dashboard	111
Annex XXXI – FraudScore prebid dashboard	112
Annex XXXII – FraudScore Pricing Plans	112
Annex XXXIII – 24metrics dashboard	113
Annex XXXIV – 24metrics helpdesk	113
Annex XXXV – 24metrics Pricing Plans	114
Annex XXXVI – Console, Mobrand's Publishing Platform	114
Annex XXXVII – OfferTest	114
Annex XXXVIII – OfferTest pricing packages	115
Annex XXXIX - SWOT Analysis	115
Annex XL – Mobile Ad Fraud Survey	116
Annex XLI – Questionnaire Responses by continents location	122
Annex XLII – “Overall, how concerned are you about ad fraud on mobile devices?”	122
Annex XLIII – “On a scale from 0-5, how would you rate the likelihood of mobile ad fraud increase in 2019? (0 being not likely at all and 5 being extremely likely)”	123
Annex XLIV – “How much of your mobile ad budget do you estimate is lost to fraud?”	123
Annex XLV – “How do you expect your company dedicated fraud prevention budget to change in 2019?”	124
Annex XLVI – Michael Porter Generic Strategies	124
Annex XLVII - Golden Triangle of Positioning of FraudProof	125
Annex XLVIII – Perceptual Map of FraudProof	125
Annex XLIX – Official logos of FraudProof	126
Annex L – Future FraudProof Website (Landing Page)	126
Annex LI – Information Flow of the FraudProof	127
Annex LII – Blacklist option	127
Annex LIII – Reporting option	127
Annex LIV – Estimated Savings Option	128
Annex LV - Pricing comparison with competitors	128
Annex LVI – Inbound Marketing Methodology	128
Annex LVII – Current organization of Mobrand	129

1. Sumário

Este projeto de mestrado pretende desenvolver um Plano de Marketing para o lançamento de uma plataforma anti-fraude online, desenhada para a indústria mundial da publicidade digital. Esta nova unidade de negócios será desenvolvida e lançada pela Mobrand, uma empresa portuguesa de tecnologia de marketing móvel.

Ao longo deste projeto, pretende-se identificar o potencial mercado desta nova linha de negócios, estudar o seu impacto para a marca e avaliar a viabilidade operacional do mesmo para a empresa em questão.

Numa primeira fase, é realizada uma Revisão de Literatura com foco nas áreas da publicidade digital, fraude digital e comércio eletrónico.

Posteriormente, é feita uma análise do mercado de maneira a identificar o valor da solução anti-fraude, sendo pesados ao longo do processo as principais oportunidades e ameaças existentes bem como os pontos fracos e fortes identificados.

De seguida, é feito um questionário para avaliar a pertinência de uma nova solução preventiva, tendo em conta a visão dos marketers sobre a fraude em publicidade *mobile* e também para entender as características mais valorizadas pelos mesmos. Tendo em conta os dados obtidos previamente, é desenvolvida uma estratégia de STP e marketing-mix que apoia a criação do sistema anti-fraude – FraudProof, adaptado às necessidades e expectativas do mercado.

Por fim, é delineado um estudo operacional que permite compreender os recursos necessários para a implementação e viabilidade do projeto.

Palavras-chave: Plano de Marketing, Publicidade Digital, Fraude Digital, Comércio Electrónico

Sistema de Classificação JEL:

- M1 Business Administration;
- M13 New Firms;

2. Abstract

This master's project intends to define and study a Marketing Plan to support the launching of a software as service anti-fraud platform designed to target the growing mobile ad-tech industry. The new business unit will be developed and launch by Mobrand, a Portuguese solution provider in the digital advertising marketplace.

Throughout this project, we aim to identify the potential market of the new business line, study its impact for the brand and evaluate its viability within Mobrand.

To achieve this, a Literature Review will be firstly executed focused on the key areas of digital advertising, digital fraud and e-commerce.

Afterwards, it will be accomplished a market analysis to identify the value of the anti-fraud solution, highlighting during the process the major opportunities and threats identified in the market, while weighing also its strengths and weaknesses.

Additionally, a survey was performed to further evaluate the pertinence of a new preventive solution taking into account marketers' view of mobile ad fraud, and also to understand the most valued characteristics. Based on the data obtained beforehand, it will be developed the STP and a marketing mix strategies that will support the creation of the anti-fraud business – FraudProof, tailored for the market needs and expectations.

Lastly, to grasp this project's viability, it will be outlined an operational viability study, which will allow us to comprehend the necessary resources to implement the project.

Key-Words: Marketing Plan, Digital Advertising, Digital Fraud, E-commerce.

JEL Classification System:

- M1 Business Administration;
- M13 New Firms;

3. Executive Summary

The present project goal is to develop and present a Marketing Plan that supports the launching of anti-fraud SaaS platform, created to help mobile advertising companies – FraudProof. This new business unit will be developed by Mobrand, a Portuguese digital advertising network.

Digital advertising recent changes have shown that big brand's marketing budgets are shifting from traditional media to digital channels, such as Google, Facebook or YouTube, as consumers also shifted their interactions to digital devices, like mobile.

As the mobile economy landscape continues to expand, user acquisition on this channel is becoming an increasingly important issue for marketers. With mobile devices seen as almost body extensions, applications are capitalizing on that growth to engage with consumers in a highly personalized way.

However, the rise of digital channel fueled, at the same time, the growth of mobile ad fraud. In 2016, the Association of National Advertisers revealed that 7.2 Billion US dollars were estimated to have been lost globally as a result of fraudulent traffic.

Understanding the true genesis of users - what is real and what is not -, is currently a competitive advantage for industry players, that are taking measures to fight the threat by adopting preventive strategies and tools. As a result, anti-fraud solutions, specifically tailored to address this topic, have become a huge business opportunity for the ones that decide to tackle the issue.

FraudProof intends to explore that breach, by developing an anti-fraud solution for companies operating in the ad tech global market whose revenue model is Cost Per Install. In order to achieve such goal, a thorough literature review will be conducted in order to understand the theoretical framework that relates with the digital advertising industry. Also, a deep comprehension of the context, in which fraud is performed, is required to understand how this new business unit intends to mitigate it. Since this anti-fraud solution will be sold and serviced online, the online channel will also be address (Software-as-a-Service) as a way to sell and provide goods and services worldwide.

Afterwards, the external environment was analyzed, through the use of PESTEL tool, to further perceive what could affect the company activity in Portugal, where it is located. The competitive environment was assessed taking into account strategic tools which allowed to identify the most impactful factors and organize potential competitors into strategic groups. Then, direct competitors and their business positioning were investigated.

After this, an analysis was carried out to frame the internal environment, detailing the company, its portfolio and way of doing business. Based on previous analyzes, a SWOT analysis was carried out to identify the main strengths, weaknesses, opportunities and threats.

Subsequently, to grasp marketers' point of view on mobile ad fraud state and to evaluate the pertinence of a new SaaS anti-fraud solution for the mobile industry, a survey was conducted. The results show that marketers are very concerned about this threat and are taking several actions to prevent it, since they are wasting important parts of their marketing budgets to fraud.

Based on data previously collected and the conclusions drawn, we defined the project's segmentation, target and positioning, followed by marketing mix strategy, which was crucial to define elements like the brand, the technological architecture, services.

According to the project's planning, the SaaS platform development should start in February 2019, being the commercial launch of FraudProof expected to happen in January 2020.

Finally, to evaluate the project's viability within Mobrand, an operational evaluation will be performed. Taking into account that the project will occur inside Mobrand's structure, its initial investment will be of 6.265€, which will be used mainly to contract more workforce and technological capacity. The investment will be financed by the Portuguese company. The assumptions of the project presuppose that FraudProof will be able to reach 196 clients in the first year. The operational analysis demonstrates that the project is economically viable. In its first year of activity, FraudProof generates a revenue of 20.868€, recovers the initial investment and achieves a profit of 14.604€.

4. Literature review

4.1. E-commerce

In 2002, Peter Drucker predicted that e-commerce (EC) would impact greatly the business as we know it. As a matter of fact, in today's world, a great deal of the exchange of valuable goods or services is not limited to the physical market. It can happen at any place, at any time, without the involved parts meeting each other by the means of a virtual marketplace.

EC can be generically defined as the "buying and selling processes supported by electronic means, primarily the Internet" (Kotler *et al.*, 2005: 135). Other definitions emerged, with some acknowledging the "use the term 'e-commerce' in a broader sense: to encompass not only the buying and selling of goods, but also the delivery of information, the providing of customer service before and after a sale, the collaboration with business partners (...)" (Napier, 2006: 2).

EC is often mistaken with e-business, that "refers to a broader definition of EC, not just the buying and selling of goods and services, but conducting all kinds of business online such as servicing customers, collaborating with business partners, delivering e-learning, and conducting electronic transactions within an organization" (Turban *et al.*, 2015:7).

There are two major types of business model – business to consumer (B2C) and business to business (B2B). Later on, EC was more detailed categorized by the type of transactions and the transacting members involved, which included other models such as business-to business-to-consumer (B2B2C), consumer-to-business (C2B), intrabusiness, business-to-employees (B2E), collaborative commerce and, lastly, e-government (Turban *et al.*, 2006).

While B2C e-commerce involves direct commercial transactions between consumers and companies, B2B e-commerce involves "transactions between and among organizations" (Turban *et al.*, 2016: 10).

Some authors have argued that marketing strategies need to be clearly distinct and separate for consumers and B2B (Coviello and Brodie, 2001). The dichotomy between these business models has been highlighted by several authors and years now. B2B market is considered to

be more fragmented and to have a long purchase cycles then B2C (Lilien, 1987). In this market, the purchase decision-making is not based on emotions or impulsive needs and desires. On the contrary, is it a strictly logical decision that normally involves more than one individual, since the transaction volume is higher comparing to B2C, thus it requires more investment. Industrial buyers are focused predominantly on performance, functionality and overall added value that the purchase will proportionate to its business and to its customers (Anderson and Narus, 1998).

As the B2B is smaller than B2C market, long-term relationships are considered key due to the importance of customer retention over time (Hakansson and Snehota, 1995).

There are three technologies that are closely connected with e-commerce: Internet of Things (IoT), Big data Analytics and Cloud Computing (Yu *et al.*, 2016). These impacted greatly the EC logistics efficiency and made possible the adoption of B2B e-commerce by small and medium-sized enterprises (SMEs), which is seen as a competitive advantage over competitors (Hamad, 2015).

Cloud, in particular, has become popular amongst online businesses due to its “versatility, storage optimization capacity, performance, 24 x 7 service availability” (Oberoi and Dey, 2017: 823).

On behalf of cloud computing technology and infrastructures, EC is considered to have entered a new era. There are three main cloud models that companies can opt for when it comes to EC logistics: infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS) (Yu *et al.*, 2016).

4.1.1. Software-as-a-Service

In 2005, Bill Gates called Software-as-a-Service (SaaS) “the next sea change” in the software business (St. Clair, 2008). SaaS can be defined as a “software deployed as a hosted service and accessed over the internet” (Carraro and Chong, 2006: 2).

The software, instead of being purchased, installed and maintained, is online, on external servers. In other words, there’s no software, no hardware. Users can access the program, from

anywhere in the world, at any time, through internet, as long as they keep paying the recurring fee of the subscription.

It is a big change from traditional software models that implied expensive setup costs, ongoing maintenance and management costs. That is why SaaS is considered very attractive for organizations – “companies and organizations can acquire software applications by subscription and outsource the management of the software infrastructure to the SaaS vendor” (St. Clair, 2008: 2).

Customers buy SaaS for numerous reasons, but mainly because they “want to minimize risk for themselves and transfer risk to their vendors” (Bouzid and Rennyson, 2015: 2).

Organizations are leaning towards cloud strategies as they “achieve enhanced scalability, a significant reduction in operating costs, greater collaboration and document control and provide ubiquitous access to their applications” (Nicholson, 2018: 8).

One cannot talk about the rise of SaaS without the rise of cloud computing. In the 1960s, these two concepts were known as “time-sharing system”. At that time, computers were so big and expensive that small and medium companies could not afford it. The need was born for the software as service industry.

SaaS started to appear more frequently in late 1990s and more evidently when Salesforce, the world’s most popular Customer Relationship Management (CRM) software, kicked off the SaaS sector (St. Clair, 2008).

Currently, there are several big known companies that rely heavily or entirely on subscription business model, such as Netflix, Spotify, LinkedIn and SaaS companies like Salesforce. “In the past decade, SaaS has been one of the fastest growing market segments and is now the third largest component of the total cloud computing industry” (Guo and Ma, 2018: 1).

Gartner predicts that cloud application services will grow 17.3% in 2019 to reach \$206.2 billion (Gartner, 2018).

4.2. Digital Advertising

“Half the money I spend on advertising is wasted, the trouble is I don't know which half.”

- John Wanamaker (1838-1922)

Almost 100 years have gone through since marketing pioneer John Wanamaker's famous quote and, ever still since then, advertising has been trying to solve the underlying efficiency challenges of an industry that aims to reach relevant people to purchase products and services at an economic rational price, avoiding wastage of time and money along the value chain.

Advertising history can be tracked back to ancient civilizations like the Egyptians or Greeks, later recognized as the first advertisers for using wall or rock paintings for commercial purposes (Zhu *et al.*, 2017). In a not so distant past, marketing was a no-brainer since advertisers had few options to choose from in it came to reaching consumers –“they could use one or more of three television networks, run advertisements in newspapers and magazines, or rely on the U.S. Postal Service and direct mail” (Fulgoni, 2015: 2).

Digital technology made advertisers' life harder since consumers no longer search for information, socialize or buy products in the same channels as they used to. Moreover, marketers are prone to face more challenges as consumers become more tech savvy thus demanding more complete digital interactions (Bughin, 2015). New approaches to reach and engage consumers were fundamental to advertising success.

The expression Digital Advertising started to appear around 1990s, after the first clickable banner went live in 1993, which led HotWired to purchase banner ads to advertise themselves (Monnappa, 2017).

Few years later, in 1997, online advertising revenue reached \$906.5 million, compared to \$267 million in 1996, according to a report revealed by the Internet Advertising Bureau (IAB). The Chairman and Senior Vice President of IAB stated – “1997 was definitely a breakthrough year for Internet advertising”. In 1999, the Journal of Interactive Marketing defended that “all marketing is, or soon will be, interactive marketing” (Lamberton and Stephen, 2016: 3).

With the burst of the “dot-com bubble”, online communities mushroomed and made possible for marketers to capitalize them as sources of information and obtain consumers insights, similar with what verifies nowadays although with more advanced media platforms such as Facebook, Twitter, Instagram, and others.

A major step in digital advertising occurred in 2000 when Google launched AdWords, which allowed advertisers to promote their ads in Google content network (Kumar, 2006). Companies now acknowledge to be deeply committed to create a “digital relationship” with customers (Phillips, 2015).

It is curious to understand that some of major keys player in our economy like Google, Facebook, Amazon and eBay did not exist twenty years ago (Kannan and Li, 2016). At this fast-moving pace, digital marketing is simply dubbed as marketing, as every strategic move a corporation might adopt involves some sort of digital aspect (Lamberton *et al.*, 2016). Hence, successful marketing is where science and art meet to deliver superior results.

Digital advertising refers to “computing platforms or systems, which use computational approaches to optimally match audiences and advertisements. In advertising ecosystems, revenue is the driving force fueling the whole systems” (Zhu *et al.* (2017: VII). One can split digital advertising into two main categories or types (Zhu *et al.*, 2017):

- 1) search advertising;
- 2) display advertising.

On search advertising, the context information is obtained after a search query provided by the user. The perfect example of these kind of ads are the kind of ads that can be found on google.com after you input a search query. The goal is to match the keywords of the search with the most relevant ads. (See Annex I – Search advertising example – Google, 2018).

In display advertising, ads are usually shown as banner ads which are displayed alongside a website’s content. Under such circumstances, the contextual information about the user is very limited although there are technical ways to match the ads with previously known information about the user (re-targeting). (See Annex II – Display advertising example – Público, 2018).

The emergence of real-time bidding (RTB) technologies made it possible “to show ads to the right person and at the right time, which implies greater effectiveness” (Estrada-Jiménez *et al.*, 2017: 34). Considered “the fastest growing area in online advertising. (...), RTB mimics stock exchanges and utilizes computer algorithms to automatically buy and sell ads in real-time” (Yuan *et al.*, 2013: 1). Before these techniques, display advertising for example trade mechanisms was based on contracts.

The rapid growth of the expenditures on this type of advertising has been steadily increasing and was expected to surpass traditional TV advertising expenditure during 2017 (Zenith Optimedia, 2017). According to PwC, in 2017, digital advertising revenue grew 21% to \$88 billion in the US, surpassing TV advertising market for the first time (PwC, 2018). The same report underlined the growth of mobile advertising that accounts for 57% of revenue (PwC, 2018). By 2019, digital spending will account for more than 50% of overall media spend (McKinsey & Company, 2015). (See Annex III – Total global spending by category (US \$ millions), at average 2014 exchange rates – McKinsey & Company, 2015). The shift to digital continues to evolve at a rapid pace. In 2017, Google’s ad revenue reached almost 95,4 billion US dollars (Statista, 2018). (See Annex IV – Google's ad revenue between 2001 and 2017 – Statista, 2018).

4.2.1. Mobile Advertising

The mobile phone has become a central piece in the lives of most consumers in a short amount of time, when compared to other consumer products (Barnes and Scornavacca, 2004). For marketers, the mobile channel presented itself as a new and innovative marketing opportunity to reach consumers anytime, anywhere, being a relevant media to build consumer-brand relationships (Friedrich *et al.*, 2009).

Mobile advertising is described as “the usage of mobile internet-based media to transmit advertising messages to consumers in form of time and location sensitive, personalized information with the overall goal to promote goods and services” (Haghirian *et al.*, 2008: 3).

As it is an extremely personal device, mobile phones are a precisely targeted communication channel, delivering effectiveness and high engagement levels when compared to other media. Several authors have highlighted the one-to-one relationships potential, between advertisers and users, that this channel foments (Leppäniemi and Karjaluo, 2005), as well as the “the

ubiquitous nature and power of mobile digital technology” that made communication with the consumer easier (Mort and Drennan, 2012: 9).

The strong presence of mobile raised furthermore the issue of user addiction - “it is a device many consumers cannot seem to do without; they always have it on and check it almost everywhere they go” (Persaud and Azhar, 2012: 418).

According to the latest forecast of Statista, the number of smartphone owners will grow from 2.1 billion in 2016 to 2.5 billion in 2019. By 2020, it is estimated that smartphones owners will be more than 6 billion (Ericsson, 2015). (See Annex V – Smartphone subscriptions per region between 2014 and 2020 – Ericsson, 2015).

According to a US research firm, companies spent \$20.8 billion in 2015 to get access to consumers via mobile apps, and \$7.9 billion via mobile browsers (eMarketer, 2015). ComScore’s 2017 U.S. Mobile App Report revealed that “mobile apps account for 57 percent of all digital media usage, and smartphone apps alone capture more than half of digital media time spent” (ComScore, 2017).

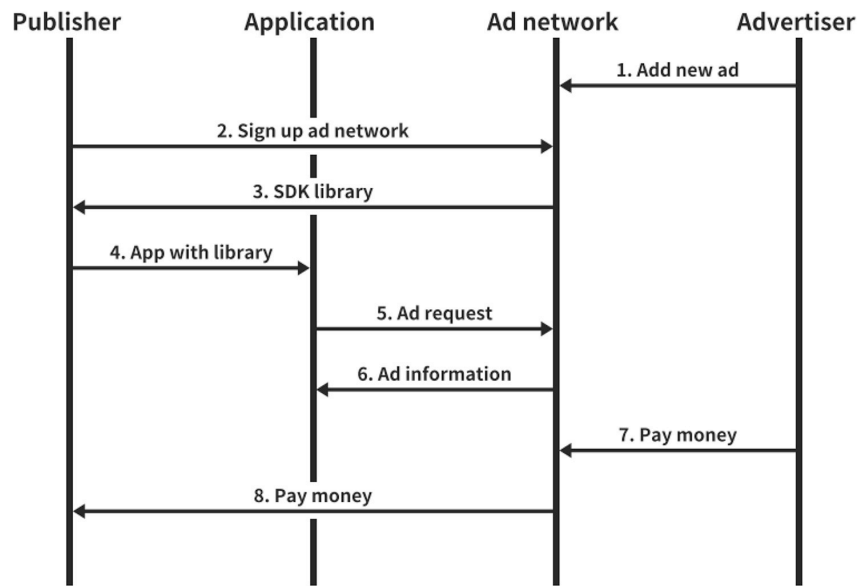
4.2.1.1. Mobile Advertising Ecosystem

Currently, the mobile advertising landscape is driven by two major forces - supply and demand (Estrada-Jiménez *et al.*, 2017), being publishers and advertisers the two main actors of the ecosystem (Haider *et al.*, 2018):

- a) On one hand, supply is represented by **publishers**, such as websites and apps, and Supply Side Platforms (SSP), that aggregates mobile inventory of thousands of publishers that want to monetize their traffic.
- b) On the other hand, we have brands, app developers, agencies and Demand Side Platforms (DSP) trying to promote their services/offers in the form of mobile ads in the publisher’s inventory. They are usually called **advertisers**, the interested part in displaying their ads, whereas publishers sell their ad inventory/space (on their websites) to increase revenue. Advertisers are interested in tracking the performance of their advertising campaign with metrics like return-on-investment (ROI) and click-through rate (CTR) (Yuan *et al.*, 2012).

Other two major type of players were further identified - ad networks and users (Yuan *et al.*, 2012). **Ad networks** are seen as moderators between the publisher and the advertiser side (Haider *et al.*, 2018). Their “purpose is to generate revenue by presenting users who browse a Publisher’s platform with relevant adverts of the Advertiser’s products and services” (Mamais, 2017: 1). Figure 1 illustrates the flow of the process that involves advertisers, ad networks, applications and publishers.

Figure 1 – Flow between ad players



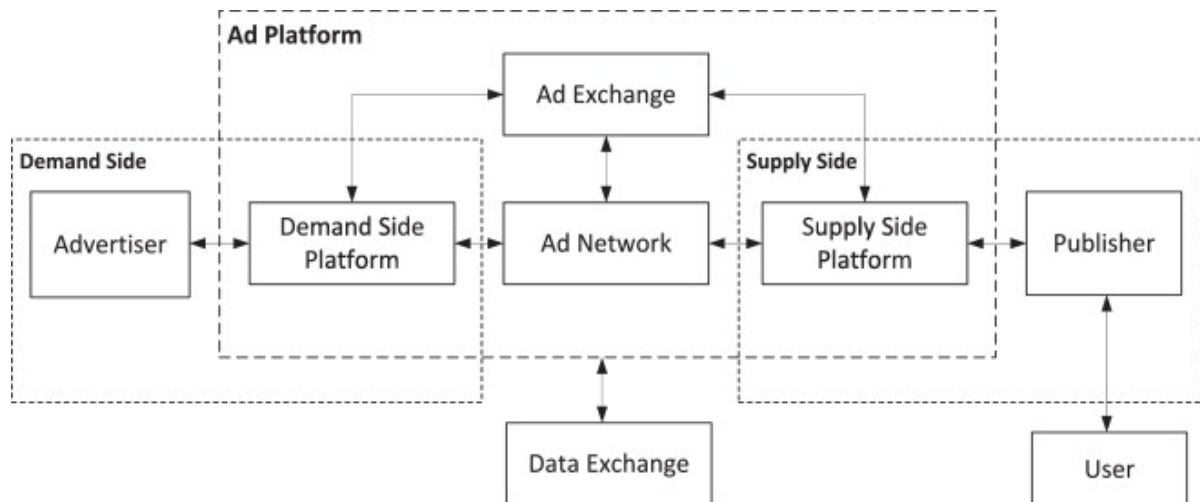
Source: Cho *et al.*, 2016

When a publisher wants to monetize its application, it must “sign up with the ad network and download the latest ad network’s software development kit (SDK) library” (Cho *et al.*, 2017: 3).

The great majority of ad networks offer Application Platform Interface (API) to publishers (Haider *et al.*, 2018). Before that could even happen, advertisers need to ask ad networks to distribute their campaigns and add those to the ad networks SDK library. When a user clicks on the ad, the application “delivers the *ad request* message containing the user device’s identifier to the ad network N. The ad network N then sends the response to the application App running on the user’s device. For that click-on-the-advertisement banner, the advertiser A pays the ad network N and the publisher P” (Cho *et al.*, 2016: 4).

This infrastructure became more intricate over the years, with more entities playing a key role to deliver personalized ads (Estrada-Jiménez *et al.*, 2017). As illustrated in Figure 2, ad platforms, ad exchanges and data exchanges joined the ad ecosystem.

Figure 2 – Advertising Ecosystem Scheme



Source: Estrada-Jiménez *et al.*, 2017

For one, **Ad platforms** are defined as “groups of entities that connect advertisers with publishers through their demand and supply-side interfaces” (Estrada-Jiménez *et al.*, 2017: 24), while **Ad exchanges** are technology platforms that collect ad spaces inventory through partnering with several entities – such as Ad networks, DSP’s and SSP’s –, and sell it by means of automated auctions. **Data exchanges** collect useful information about internet users to aid demand and supply entities targeting decisions (Estrada-Jiménez *et al.*, 2017).

Another important player in the ecosystem are **Attribution Providers**, that act as attribution credit regulators. IAB defines attribution as “the process of identifying a set of user actions (‘events’) across screens and touch points that contribute in some manner to a desired outcome, and then assigning value to each of these events” (IAB, 2016). It is attribution that tracks the user’s journey from click to in-app activity.

According to Appsflyer, attribution providers are considered impartial since they do not buy or sell mobile ads, and thus are trusted by both sides of the equation “to measure and report on campaign performance”. These companies normally are able to connect attribution with in-app activity, which provides marketers with valuable analytics and insights about which

source delivered the expected results (engagement, return on investment, lifetime value, retention rate).

4.2.2. Revenue Models

To get the best possible customers across the internet, marketers started to buy media programmatically, achieving better results, greater scale and more control over price. In general, there are three major business models in mobile advertising— cost per *mille* (CPM), cost per click (CPC) and cost per action (CPA) (Cho *et al.*, 2016).

In the early days of internet advertising, ads were first sold on CPM, the pricing model where “the advertiser was charged proportionally to the number of times the ad was displayed on a web page” (Ratliff and Rubinfeld, 2010: 3). As the name states, the advertiser pays for 1000 displays of their mobile ads. This payment model has a downside and has been under scrutiny since “the advertiser is forced to pay for all displayed advertisements regardless of whether they were actually seen by the consumer or not” (Matin, 2007: 537).

CPM was the leading model until Procter&Gamble negotiated with Yahoo! in 1996 the promotion of ads on its website based on CPC, a performance-based pricing model. Yahoo! was paid every time a user clicked on the ad (Evans, 2009). Search engines, like GoTo.com, made CPC pricing more appealing by the means of auctions.

CPC is considered the most popular revenue model (Mamais, 2017), but its leadership is being disputed by CPA, a new performance-based model (Hu *et al.*, 2013). Marissa Mayer, former president and chief executive officer of Yahoo, called CPA the “Holy Grail” for targeted advertising (Hu *et al.*, 2013). In the CPA model, the advertiser is charged for a more elaborate action, such as a lead or a sale (Cudmore *et al.*, 2009). This model “allows the advertisers to report their payoff after observing the user’s action; therefore, it eliminates the uncertainty of advertisers and reduces their exposure and computational burden” (Nazerzadeh, 2013: 99).

With the rise of the mobile app economy emerged a model focused on user acquisition – cost-per-install (CPI). This advertising model “is a type of performance-based model or CPA advertising which includes the popular CPC” (Chiong and Chen, 2016: 6). In this revenue

model advertisers are charged only when a click on their ads results into an actual mobile app install.

Usually, CPM and CPC models are targeted for branding campaigns in which there isn't a direct way to measure performance. Thus, these models are usually transacted on real-time-bidding systems. Simply put, RTB is the buying and selling of ad impressions by means of an auction that occurs in the time it takes a webpage to load (Bush, 2015). While the impression loads, data about the user is transmitted to the advertisers. If interested, they will start the bidding process. On the contrary, traditional advertising media don't support RTB, and the value to pay for the ad are negotiated before the ads are shown (Yuan *et al.*, 2012).

CPA models, on the other hand, are considered strict performance based campaigns because the advertiser will only be charged if there is a successful action/transaction, being transacted via Performance Based Networks. The advertiser has a positive return on investment when legitimate impressions, clicks and actions are generated by real users. More recently, hybrid models, which are created through the combination of models, e.g. CPM+CPC, CPM+CPL, become more popular since those provide more security to the advertiser and guarantee more profit for the publisher, when key performance indicators (KPI) are reached (Rzemieniak, 2015).

4.3. Digital Fraud

Since the launching of internet, fraud has been a major concern, with digital advertising being its much-loved victim (Fulgoni *et al.*, 2016). When marketers buy advertising, they demand and expect human interactions, but more often than not what they are getting in return are bots interaction - improved and more human-like every day. Which raised the following question - "If an advertisement runs online and no one sees it, is it still an ad?" (Flosi *et al.*, 2013: 1).

Digital fraud can be described as "any (malicious) activity that hampers the advertiser's plan to draw a desired number of customers from the money he is willing to pay in advertising, can be termed as an ad fraud" (Haider *et al.*, 2018: 128).

The World Federation of Advertisers portrays ad fraud as an organized crime, surpassed only by the drugs trade, that will cost advertisers \$50 billion a year by 2025 (World Federation of Advertisers, 2016).

A concern for this industry is that almost 30% of the revenue generated by digital advertising is channeled for bots that “simulate impressions and clicks in such a way that the generated traffic resembles real traffic as much as possible” (Rajab *et al.*, 2006: 41).

In 2017, Google removed 40 apps of its Play store, that allegedly had been downloaded 36 million times. In reality, the apps were forcing android users to illegitimate click on ads in the background, through a software (Forbes, 2017). Android is considered more likely to suffer from fraud – “mobile users are increasingly becoming targets of malware infections and scams. Some platforms, such as Android, are more open than others and are therefore easier to exploit than other platforms.” (Rastogi *et al.*, 2016: 1).

According to comScore study, 52% of digital campaigns are out of view to humans or subject to fraudulent and invalid traffic, whilst less than half is viewable by humans (comScore, 2016). (See Annex VI – Percent of U.S Digital ad impressions by viewability and non-viewability – comScore, 2016).

The development of advertising platforms and technology innovation however was not escorted by fraud prevention solutions, which didn’t allow the “digital marketing industry to reach full potential” (Fulgoni *et al.*, 2016: 199). Several authors stress that while web advertising has been studied thoroughly, the same cannot be said about mobile ad fraud (Haider *et al.*, 2018; Dong *et al.*, 2017). The present state has much to do with the fact that digital advertising technology underlying foundations were not designed with fraud prevention in mind (Zhu, 2017).

In the fight against ad fraud, advertisers don’t lose just money, but also trust in digital media. Still, not all fraud is bot generated. A significant percentage of fraud is actually human traffic (Vidakovic, 2015). Moreover, fraudulent activity can be perpetrated by the most interested in fighting ad fraud – “the fraudster may be a publisher in the exchange who is attempting to make more money than it deserves, or an advertiser who is targeting other advertisers to reduce ad competition” (Stone-Gross, 2011: 281).

A report from Hewlett Packard investigated the business of hacking and classified ad fraud attractiveness based on financial gain and effort as providing the highest profit with the least amount of effort and risk (Hewlett Packard Enterprise, 2016). (See Annex VII – Attractiveness of hacking based on effort and profit – Hewlett Packard Enterprise, 2016).

Many ad networks and ad tech providers lead the area in identifying, cataloguing, analyzing mobile ad fraud in order to develop methods to prevent and block fraudulent events before they even begin.

As the mobile ad industry continues to grow so do fraudsters and their techniques. Nowadays, fraudulent activity can be triggered at any stage along the conversion funnel, from impression to click, install and post-install events.

The ad tech company AppLift distinguishes two main types of fraud: technical fraud which can be defined as “fraud committed through the use of technology to ‘game’ the ad tech system” and compliance fraud which can be described as “deceitful tactics that do not directly require any specific kind of technology but aim to exploit platform vulnerabilities” (AppLift, 2015: 7).

However, other authors have associated the revenue model with the type of fraud: “each of the ad revenue models (...) (impression-based, click-based, and action-based) can be subject to corresponding types of spam” (Daswani *et al.*, 2008: 8).

Impression spam is considered the easiest kind of fraud because “involves fabricating HTTP requests to either the publisher’s page, or the ad server directly, to artificially inflate the actual amount of traffic” (Stone-Gross *et al.*, 2011: 281).

CPM campaigns are 3 times more likely to attract fraud compared to CPC offers and 10 times more likely to attract fraud than CPI campaigns (Applift, 2015). A report from the mobile ad company StartApp states that the most common impression fraud tactics are ad stacking, invisible pixels, “unstoppable” apps and video auto-play (StartApp, 2017).

The CPC system, for once, has also disadvantage, since it is “highly susceptible to a particular style of fraudulent attack called click fraud” (Immorlica *et al.*, 2005: 34). Click fraud is “arguably the cyber-world’s biggest scam” (Kshetri, 2010: 45), and takes place “when illegitimate sources click on online ads with a malicious intent”, being botnets the most severe form of click-fraud (Iqbal *et al.*, 2016: 157).

Click farms, generated by human viewers, and click bots, generated by computer programs, are the main two types of click fraud (Zhu *et al.*, 2017). Several companies in the industry further delve deep into the categorizing types of click fraud and added more varieties - click stuffing, click redirection, click spamming, click injection and clickbait (StartApp, 2017).

Due to its cost-effectiveness, CPA became popular amongst online advertisers but this model is also susceptible to fraud. CPA fraud “intends to target users’ meaningful business actions, such as filling an online form or survey, placing an online purchase order, or use users’ previous actions or behaviors to re-target valuable customers” (Zhu *et al.*, 2017: 33).

This model is also known due to higher chances of advertiser fraud – “since the publisher (and the commissioner, if he exists) have no way to confirm whether or not a specific action has taken place they depend on the advertiser to report the customer’s action truthfully” (Soubusta, 2008: 140). CPA is considered less vulnerable to attacks than CPC and CPM since it is more expensive to generate a fraudulent action (Nazerzadeh *et al.*, 2008). Install fraud is the most prevalent form of CPI, the most common pricing model in performance app marketing (Appsflyer, 2016).

5. Conceptual Reference Framework

Taking into account the most relevant aspects and inputs gathered from the Literature review, a conceptual framework of reference will be outlined in a synthesized manner. These will be fundamental further along the project, when defining strategic approaches to the market and defining marketing mix.

Table 1 – Conceptual Framework of Reference

Subject	Description
Digital Advertising	The shift from traditional media to digital media is evolving at a rapid pace. By 2019, digital spending will account for more than 50% of overall media spend (McKinsey & Company, 2015). With such growth, digital marketing will be simply dubbed as marketing, as every strategic move a corporation might adopt involves some sort of digital aspect (Lamberton <i>et al.</i>, 2016). In parallel, marketers are also prone to face more challenges as consumers become more tech savvy thus demanding more complete digital interactions and experiences (Bughin, 2015). The rising of digital advertising landscape potentialized user acquisition in this channel, which drove the emergence of technologies like real-time bidding. RTB was a game changer as it allowed to show ads to the desired target at the desired time achieving high levels of effectiveness (Estrada-Jiménez, 2017).
Mobile Advertising	Mobile phone has become a central piece in the lives of most consumers in a short amount of time, when compared to other consumer products (Barnes and Scornavacca, 2004). Several authors highlighted the one-to-one relationships potential, between advertisers and users, that this channel foments (Leppäniemi and Karjaluo, 2005). For marketers, the mobile channel presented itself as a new and innovative marketing opportunity to reach consumers anytime, anywhere, being a relevant media to build consumer-brand relationships (Friedrich <i>et al.</i>, 2009). By 2020, it is estimated that smartphones owners will be more than 6 billion (Ericsson, 2017). The strong presence of mobile raised furthermore the issue of user addiction (Persaud and Azhar, 2012: 418).
Mobile Ad Ecosystem	Mobile advertising landscape is driven by two major forces - supply and demand (Estrada-Jiménez <i>et al.</i>, 2017), being publishers and advertisers the two main actors of the ecosystem (Haider <i>et al.</i>, 2018). Other two major type of players were further identified - ad networks and users (Yuan <i>et al.</i>, 2012). There are three major business models in mobile advertising– cost per <i>mille</i> (CPM), cost per click (CPC) and cost per action (CPA) (Cho <i>et al.</i>, 2016).
Digital Fraud	Since the launching of internet, fraud has been a major concern, with digital advertising being its much-loved victim (Fulgoni <i>et al.</i>, 2016). Almost 30% of the revenue generated by digital advertising is channeled for bots that “simulate impressions and clicks in such a way that the generated traffic resembles real traffic as much as possible” (Rajab <i>et al.</i>, 2006:41). The development of advertising platforms and technology innovation however was not escorted by fraud prevention solutions (Fulgoni <i>et al.</i>, 2016). According to Zhu (2017), the digital advertising technology foundations were not designed with fraud prevention in mind, which allowed its proliferation. According to Daswani <i>et al.</i>, (2008), to which of the ad revenue model corresponds a type of fraud. With the technological

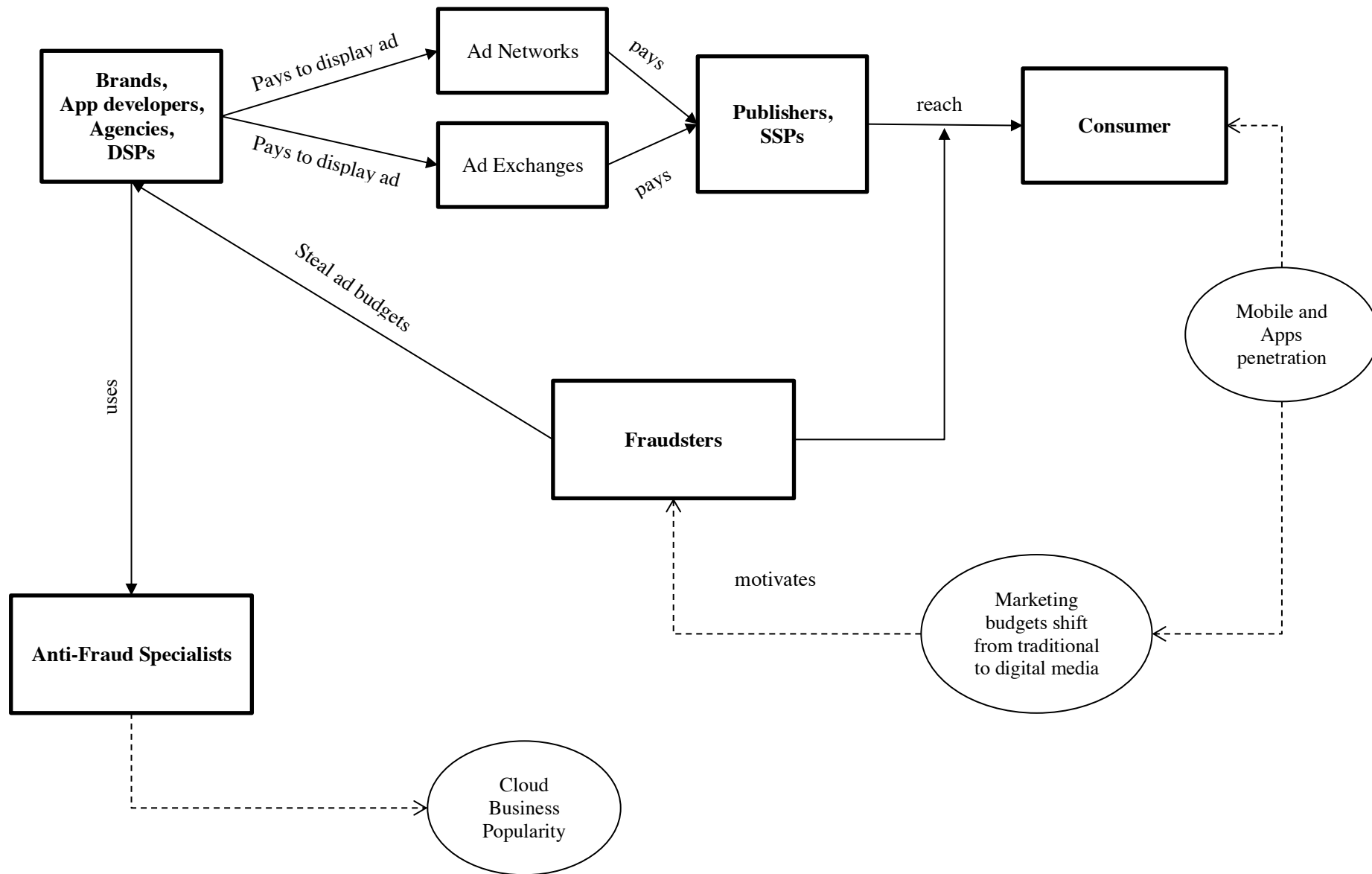
	advances, fraudulent activity can be triggered at any stage along the conversion funnel, from impression to click, install and post-install events.
E-commerce	In today's world, a great deal of the exchange of valuable goods or services is not limited to the physical market. It can happen at any place, at any time, without the involved parts meeting each other by the means of a virtual marketplace. There are two major types of business model – business to consumer (B2C) and business to business (B2B) (Turban <i>et al.</i>, 2016). For the purpose of this project, the B2B is the appropriate market. B2B market is considered to be more fragmented, to have a long purchase cycles then B2C (Lilien, 1987), to require long-term relationships (Hakansson and Snehota, 1995). Directly linked with e-commerce is cloud computing, as stated Yu <i>et al.</i> (2016), which impacted greatly the EC and B2B logistics. According to Oberoi and Dey (2017), cloud computing technologies have become popular amongst online businesses as it is versatile, has good storage capacity, performance and high availability. By the end of 2022, cloud services are expected to worth \$164.3 billion (Transparency Market Research, 2018). There are three main cloud models that companies can opt for when it comes to EC logistics: infrastructure as a service (IaaS), Platform as a service (PaaS) and Software as a service (SaaS) (Yu <i>et al.</i>, 2016). SaaS model has become very attractive for B2B online businesses since it allows users to access the software, hosted in external serves, via the internet. There is no software or hardware. This permits to save setup, maintenance and management costs, while minimizing risk for the businesses.

Source: The Author, 2018

Figure 3 illustrates in a concise way how the ecosystem works and communicates. On one side, we have brands, app developers, agencies, DSPs that are paying ad networks and ad exchanges to promote their ads alongside consumers. These mediators, for once, are paying direct publishers and SSPs to promote those ads, thus monetizing their website/app space inventory. The growing popularity of mobile advertising together with mobile and apps penetration drove the rise of the phenomenon of mobile ad fraud, which altered the landscape completely. Fraudsters are taking advantage of marketing budget shift from traditional to digital media, stealing large portions of ad resources. The emergence of mobile ad fraud created a hole in the app economy, generating a new business opportunity for anti-fraud specialists.

At the moment, marketers are working directly with those companies to develop effective fraud prevention and detection strategies and regain competitive advantage. At the same time, cloud computing technologies supported the take-off of anti-fraud specialists. Its scalability, 24/7 worldwide availability and, overall, less upfront costs made cloud popular specially in B2B businesses like these.

Figure 3 – Synthesis figure of Literature Review



Source: The Author, 2018

6. Data collection and methodology

The following table describes the research methods used in order to obtain valuable insights for the project. The market research was divided in primary data and secondary data.

As primary source of research methodology, a survey will be conducted in order to understand marketers perception of the mobile ad fraud ecosystem and, furthermore, apprehend their insights and most valorised elements during the design of a new anti-fraud solution.

We also obtained secondary data of two types: internal and external data. To obtain internal data, we used information provided by Mobrand, whose contribution was significant. To obtain external data, we used data from INE, Marktest, Eurostat, Statista, OCDE, PORDATA and AICEP.

Table 2 – Market Research Data

Classification	Type	Source
Primary Data	External Data	Survey
Secondary Data	Secondary Data	Mobrand
	External Data	INE
		Marktest
		Eurostat
		Statista
		OCDE
		PORDATA
		AICEP

Source: The Author, 2018

7. External Analysis

7.1. PESTEL Analysis

7.1.1. Political - Legal

In March 2016, Marcelo Rebelo de Sousa, a veteran of the center-right Social Democratic Party, won Portugal's presidential election. The current government is led by António Costa, the socialist party leader that was able to form a PS minority government in October 2015, with the support of the two far-left parties in parliament. Even though Europe's left is struggling at the moment, Portugal's government alliance is achieving stability.

Legally, the current Portuguese legislation does not impose itself major impact to the digital advertising industry. Marketing legislation is diverse in Portugal, being Advertising Code and the Law of Electronic Commerce the most recognizable ones. The supervisory entity is the Autoridade Nacional de Comunicações (ANACOM).

The rising of e-commerce regulation could pose as a threat – by imposing stricter requirements and regulations -, but also an opportunity for companies – to expand globally.

The latest development in this area was taken by the EU when regarding data privacy, by approving the General Data Protection Regulation (GDPR) (EU 2016/679), which became law on May 25, 2018.

The GDPR applies to all the organizations that offer products or services to European consumers, regardless of the company's location. The European law gives power to citizens over their personal data and new obligations for companies, across all business sectors, that handle EU data.

As a member of the EU, Portugal needs to be compliant with the new data protection laws. If companies fail to meet the requirements, they could will face heavy fines – up to 4% of annual global turnover.

7.1.2. Economic

After receiving a 78-billion-euro international bailout in 2011, Portugal shifted from a financial crisis to a path of economic recovery. The year of 2014 recorded the first signs of recuperation, after three years of contraction.

Between 2006 and 2016, the average growth rate of the Portuguese GDP was of -0.2%, while the Euro Area (EA) and the European Union (EU) maintained positive values, with an average GDP growth of 0,5% and 0,7% respectively (Eurostat, 2017). (See Annex VIII – GDP growth in the EU-28 during 2006 and 2016 – Eurostat, 2017)

In 2009, the global economic and financial crisis had a negative impact on the members of the EU-28 and EA-19, whose real GDP growth rate fell to -4,4% and -4,5%, respectively. It is possible to conclude that the Euro Zone economic climate also has an influence on the Portuguese economic.

The Portuguese GDP increased 2,7% in 2017, achieving 193,1 billion euros in nominal terms. In the first trimester of 2018, GDP is expected to grow 2,1%, in line with European economy evolution (INE, 2018). (See Annex IX – GDP evolution between 1996 and 2017 – INE, 2018).

In 2018, the Portuguese economy should get back to the pre-crisis levels of 2008, according to Banco de Portugal. The economy growth has been followed by a continuous fall in the unemployment rate that is currently at 6,7%, the lowest value in more than decade (INE), and below EU28 and EA19. The increase in employment will have an impact in the unemployment rate that is expected to reach 5,6% by 2020 (Eurostat, 2018). (See Annex X – Unemployment rate in member states of the European Union in June 2018 (seasonally adjusted) – Eurostat, 2018).

Recently, in April 2018, Portugal registered the third lowest annual inflation rate (0,3%) in the European Union, according to Eurostat. The indicator also slowed down in the EU28 (1,4%) and EA19 (1,2%).

The most punished sector by the crisis was the construction, that started to recovery slightly during 2016, but it is still far from 2008 levels. In 2005, this sector was responsible for 6,6% of Gross Value Added (GVA) and 10,7% of employment. Between 2002 and 2016, the Gross Value Added (GVA) of the construction decreased 53% (INE, 2016).

The EU28 and EA-18 also saw the construction production drop drastically in 2008. (See XI – EU-28 Construction, annual rate of change 2005-2017 – Eurostat, 2018). In another countries, construction production experience reductions before 2009. It is the case of Portugal that went on a downwards spiral, achieving a reduction of -16.2% in 2013.

Tourism, on the other hand, has been breaking records in the past years and has been contributing like never before to the national economy. The total contribution of travel and tourism to Portugal's GDP reached 17.3% (33.5 billion euros) in 2017. It is expected to reach 20.5% of GDP in 2028 (World Travel & Tourism Council, 2018). (See Annex XII – Total attribution of Travel and Tourism to Portugal GDP – World Travel & Tourism Council, 2018).

Tourism is the largest employer of the country, employing almost 1 million direct and indirect jobs, being Portugal also in the top five most-visited countries in Europe (World Travel & Tourism Council, 2018).

Similarly to neighbor European countries, the structure of the Portuguese economy is characterized by the strong weight of the services sector, that employed 68.6% of the population in 2016 and has accountable for 75.4% of GVA (AICEP, 2017) (See Annex XIII – Portuguese GVA distribution in 2016 – INE, 2017; Annex XIV – Employment distribution – INE, 2017).

7.1.3. Social

According to PORDATA, in 2016, Portugal had 10.325 million inhabitants, including the mainland and the archipelagos Madeira and Azores. The evolution of the Portuguese population has been accompanied by a progressive ageing of the population, due to falling fertility rates and to the increase of life expectancy. In addition to these factors, the increased emigration also played a role in structure of the Portuguese population.

Recent data from the INE reveals that the Portuguese population decreased in 2017, by the ninth consecutive year, since the number of deaths is still higher than the number of births. INE projects that Portugal will lose population year by year, reaching 7.5 million people in 2080, with the working age population declining from 6.7 to 3.8 million people.

The EU's Eurostat agency predicts that Portugal will be the EU country with the smallest proportion of children, with the percentage of under-15s dropping from 14.6% in 2014 to 11.5% in 2050.

Looking into the evolution of the demographic pyramid, it is possible to see the narrowing of the base of the age pyramid, which translates into less young people – due to low birth rates –, and the enlargement of the top of the pyramid, which translates into more elder people –due to the increase in longevity. (See Annex XV – Portugal Age Pyramids 2011, 2016 and 2080 (projection) – INE, 2016).

These transformations can also be observed in the EU-28's population structure. Projections indicate that by 2080, in the EU-28, there will be 66.1 million people aged 80 years (Eurostat, 2017). Annex XVI shows clearly the changes in the EU-28's population, by overlapping two pyramids that concern the changes by age and sex for 2016 and 2080. (See Annex XVI – EU-28 age pyramids, 2016 and 2080 (% of total population) – Eurostat, 2017). Overall, it projects the same phenomenon that is also happening in Portugal: low number of births, less working age population, ageing population.

While Portugal is amongst the list of the countries with highest decline in the total numbers of inhabitants by 2080, United Kingdom, France and Germany will be the largest EU members in terms of population (Eurostat, 2017).

Before 1991, Portugal did not have access to phones. Today, is hard to find someone who does not possess one due to intense development of telecommunications and the consequent massification of such devices.

Mobile devices - such as smartphones or tablets –, have become a part of people's daily lives, facilitating access to internet and creating the necessity of being always connected.

Two thirds of teenagers feel a “great necessity” of checking their phone constantly to see if something happened and more than half have felt bored if incapable of using those devices due to lack of battery or network. These are some of the conclusions of the project Net Children Go Mobile (2014), of which Portugal is also part and also points out the overuse of technology by young people.

When comparing excessive usage of smartphone with other seven European countries, the study also found that the Portuguese children and teenagers present a higher value (57%) than the European average (48%), being surpassed only by the United Kingdom (65%).

A research from the Instituto Universitário de Ciências Psicológicas, Sociais e da Vida (ISPA, 2014) concludes in the same direction – almost $\frac{3}{4}$ of the Portuguese population, aged up to 25, has signs of digital addiction. Amongst respondents, almost $\frac{1}{4}$ revealed high levels of social isolation.

Eight out of ten Portuguese teenagers with 15 years admitted “feeling bad” if they are not connected to the internet, according to 2015 OCDE data about 31 countries (OCDE, 2018). Electronic media consumption starts at an early stage in the Portuguese households, being tablets and smartphones used by parents to calm and distract children (ERC, 2017).

7.1.4. Technological

From a technological point of view, internet penetration continues to grow in Portugal with 5,9 million users (Marktest, 2017), despite remaining below EU average. It is expected to reach 86% by 2020, coming close to Europe’s share (Eurostat, 2015).

In 2016, 85% of the EU-28 households had internet connection (Statista, 2017). Forecasts indicate that the UK is expected to reach 95% internet penetration in 2021, followed by France (81.32%) and Germany (82.62%).

Portugal is amongst the countries that registered a rapid expansion in what concerns the proportion of households with access to internet, between 2012 and 2017. (See Annex XVII – Internet Access of households between 2012 and 2017 (% of all households) – Eurostat, 2018).

There is an urban-rural gap in the EU-28 regarding internet access. Households in cities or towns/suburbs registered high access rates, 90% and 87 respectively, while rural areas had a lower value – 82% (See Annex XVIII – Internet access in households by degree of urbanization 2017 – Eurostat, 2018). Portugal is amongst the EU countries where the gap between rural areas and urban is particularly clear (Eurostat, 2018).

Portugal ranked 16th out of 28 countries in the European Commission's Digital Economy and Society Index 2018 (DESI, 2018). Portugal's biggest challenge is related with the digital skills levels of the Portuguese population.

In 2007, Portugal had 12,9 million cell phone users, according to Association of Communications and Telecommunications (ANACOM), a higher number than its population: 10,3 million (INE). Smartphone penetration is around 70% in Portugal (Marktest, 2017).

In 2016, Portugal was the third country in the European Union with more mobile phone service subscriptions per thousand inhabitants (PORDATA, 2016). (See Annex XIX – Subscribers of the mobile service per thousand inhabitants in 2016 – PORDATA, 2016)

In 2017, 77% of the Portuguese families had access to internet at home, being 76% of the connection made by broadband (INE, 2017). Despite the increase, the broadband penetration among Portuguese families remains low when compared to the average UE families. (See Annex XX – Proportion of households with broadband internet at home - Portugal and EU28, 2010-2017 – INE, 2017). Internet usage rates are also linked to education, being higher for those who have completed high school (97%) and college (99%) (INE, 2017).

In 2017, 34% of Portuguese population - between 16 and 85 years old – reported using the internet to order products or services. The substantial increase, however, falls short when comparing to the EU-28 average that stood in 55% in 2016. (Annex XXI – Proportion of people with 16 and 74 years old using e-commerce in Portugal and EU, 2010-2017 – INE, 2017).

The e-commerce market is growing, with more clients using their devices to purchase online, making companies invest in their online presence. In 2017, it is estimated that 1.66 billion people worldwide bought goods or services online (Statista, 2017). The value of online

shopping reached 4.6 billion euros in 2017 and should achieve 8.9 billion by 2025, according to a Digital Economy study (ACEPI, 2018).

Accessing internet on the move, while using a portable device, is a growing trend in Portugal – in 2017, 79% of internet users connected to the internet while using a portable device, specially the smartphone (76%) (INE, 2017).

7.1.5. Environment

Nowadays, companies face the threat of climate change which could ultimately affect the business performance. In Mobrand's case, the environmental factor poses a threat to the physical structure of the company – in case of climate change, availability of energy, for example -, and could eventually lead the company to transfer their servers and other equipment to another place.

The direct environment impact of an e-commerce industry is considered to be low, still companies are embracing heavily sustainability strategies. Mobrand could put in practice a business strategy that prioritizes green, renewable and sustainable technologies to create a more efficient workplace.

8. Competitive Analysis

8.1. Five Forces of Porter Analysis

The Five Forces of Porter framework is a useful tool to better understand the attractiveness of the mobile advertising industry when it comes to address fraud solutions.

The model, named after Michael Porter states that there are five forces that assess the overall competitive intensity and attractiveness of a particular industry. Those are Bargaining Power of Buyers, Bargaining Power of Suppliers, Threat of New Entrants, Threat of Substitutes and Industry Rivalry.

In the following analysis, it was defined a set of factors that have a direct impact in the power of each of the competitive forces identified by Porter, in 1979. Each factor was scored in a nominal scale from one to five, with one representing the lowest threat and five representing the highest threat. Following that, an arithmetic mean was calculated to score the power of each of the forces.

8.1.1. Industry Rivalry

- Existence of several companies operating in the mobile advertising industry (moderate fragmentation)
- Existence of few anti-fraud solutions in the mobile advertising industry
- The main competitors are international companies that operate at a global scale
- The major companies operating in this industry have a strong brand image and credibility that is internationally recognized
- The existent companies follow similar strategies, sometimes with different business models, segments and value propositions
- Medium to high exit costs, depending on the type of tech structure
- Existing companies have skilled manpower
- The optimistic industry growth makes the atmosphere competitive

Power level: 3.6 (High)

Foreign competitors play a major key role in the mobile ad industry, offering a wide range of anti-fraud solutions, each one pursuing diverse market-target. Even though it is difficult to

calculate the potential number of clients of anti-fraud tool, given the overall industry fragmentation and its electronical distribution component, it is safe to say that there are dozens of anti-fraud players, working at a global scale in the mobile advertising industry. These companies are perceived to have strong brand image and credibility by the other players in the industry, since the majority specialized its services solely on fraud detection and prevention technologies.

Depending on the type of technologic structure chosen, rivals might have medium to high exit costs. Outsourcing services could, for instance, impose a fee payment before the end of the contract.

Overall, the existent of strong and established players and the possibility of diversification of companies of the mobile ad industry are the two main factors affecting industry rivalry, that represents a high power – (3.6).

8.1.2. Threat of New Entrants

- Time and entry cost (R&D, technology wise) is very high
- Entry demands specific know-how
- High branding and advertising costs to create market awareness and customer loyalty
- Relationship-based business
- Access to suppliers (servers and storage) do not represent a barrier to entry
- Diversification possibility from existing companies in the industry

Power level: 2.9 (Medium)

The threat of new entrants into the mobile advertising industry is not that likely as the startup cost of entering this market translates into a high investment in time, R&D, technological, human resources and, also, relationship wise. So, there is a journey ahead before being recognized as a respectable competitor within the landscape of the established companies.

Taking into account the growing and competitive atmosphere, it is likely that mobile ad companies try to diversify their services/products. This means that the potential buyers could be a potential entrant if they decide to invest internally in an anti-fraud tool, as other companies already did. It would be easier given that they already possess skilled manpower in

the area and that their developing costs would be substantially lower compared to a new company.

Besides that, there are no legal barriers or protectionist policies that might hinder the entry of new players in the Portuguese market. It is important to underline that the easy access to the necessary technology (servers, software licenses, etc.) facilitates the entry of new players in the market. Overall, the threat of new entrants in the industry is medium (2.9).

8.1.3. Bargaining Power of Suppliers

- Bargaining power of suppliers remains relatively high, even though new players are starting to compete with the big players
- Cloud storage space price decreased greatly due to the increased competition in providing the same service
- There are limited suppliers with good value propositions
- Technology hardware infrastructure has relatively low fixed costs
- Existence of good substitutes
- Low to medium switching costs

Power level: 3.2 (Medium)

Since there are not a lot of suppliers offering good quality services in the industry and that the volume of purchase do not represent a large portion of the supplier's sales, the bargaining power of suppliers is high.

However due to the democratization of information on big data and machine learning, there are new players starting to emerge in the industry, competing with the key ones, dropping the prices on technology hardware infrastructure and also software. There is also no threat of forward integration by the suppliers and low to medium switching costs.

Considering skilled workforce as suppliers, one must add that the current Portuguese market has a shortage of tech workers, which may hamper the task of finding those workers with the necessary skills in time. The bargaining power of suppliers is considered medium (3.2).

8.1.4. Bargaining Power of Buyers

- Medium number of buyers;
- Medium to high transactions per month, depending on the pricing package chosen and buyers' needs;
- Buyers have a lot of information about anti-fraud ad solutions available in the market;
- Low or high switching costs depending on the type of packages chosen (pay as you go, monthly or annual package, etc.)
- Sellers are available globally via internet;

Power level: 3.2 (Medium)

Since this industry is B2B, the companies (networks, exchanges, SSPs, DSPs, app developers) that operate in the mobile advertising industry are considered the main buyers. In the Portuguese market, the number of buyers is relatively low, being the higher volume of customers in the international market.

The buyers have a lot information about the established competitors and their unique selling propositions (how they monitor mobile ad campaigns, detect malicious activity and eliminate fraudulent sources; if they integrate with trackers or platforms, for example).

Buyers can choose from several pricing schemes that depend mostly on the volume of data processed monthly (click, install), being the great majority purchased on a monthly basis, with no commitment. However, there that are players that offer friendly annual discounts. So, moving to another supplier could have either non-exist to high costs.

Thus, the bargaining power of buyers is medium (3.2).

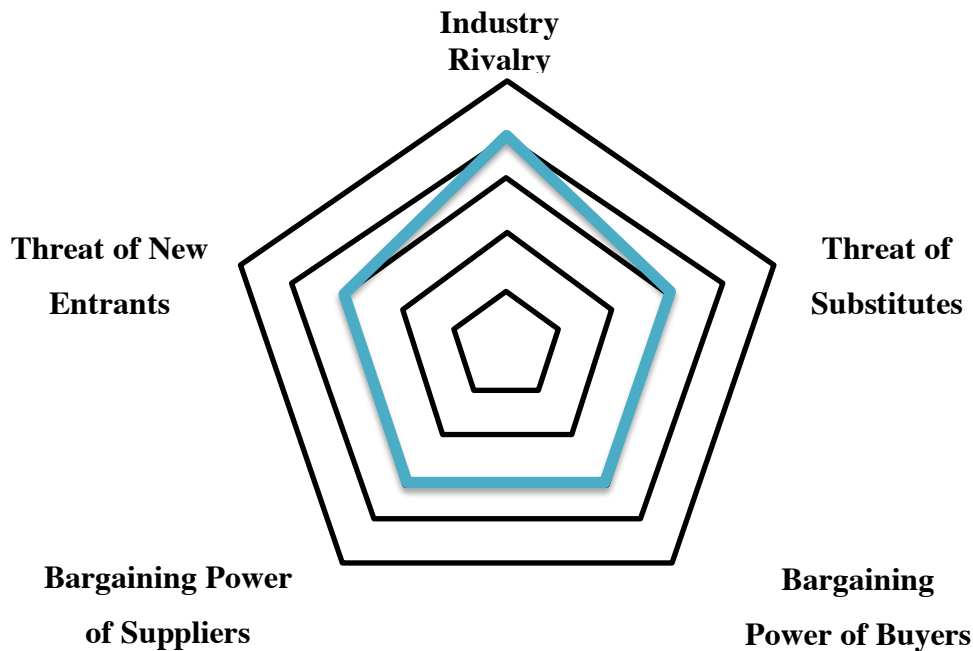
8.1.5. Threat of Substitutes

- Existence of substitute for the industry service (known attribution platforms that offer add-ons, for example);
- Non-existent to high switching costs to other services and products;
- Buyers tend to become loyal if their losses to fraud decrease;
- Price-performance ratio is low.

Power level: 2.8 (Medium)

The threat of substitutes is medium since there are several substitute services starting to arise in the landscape. For example, industry leaders for mobile attribution are also leading the fight against mobile ad fraud and have been developing tools to complement their platform. Once more, switching costs could be non-existing or high, depending on companies and pricing strategies practiced. There are vendors that charge a large fee if marketers want to migrate their current data infrastructure to another platform. If they want to avoid data losses, marketers are not able to dodge switching costs. However, their price-performance ratio is considered to be low, since it is considered an add-on to the business main service.

Figure 4 – Industry Attractiveness: 5 Forces of Porter



Source: The Author, 2018

Table 3 – Level of the forces in the industry

Force	Level
Industry Rivalry	3.6
Threat of Substitutes	2.8
Threat of New Entrants	2.9
Bargaining Power of Buyers	3.2
Bargaining Power of Suppliers	3.2
Mean	3,1

Source: The Author, 2018

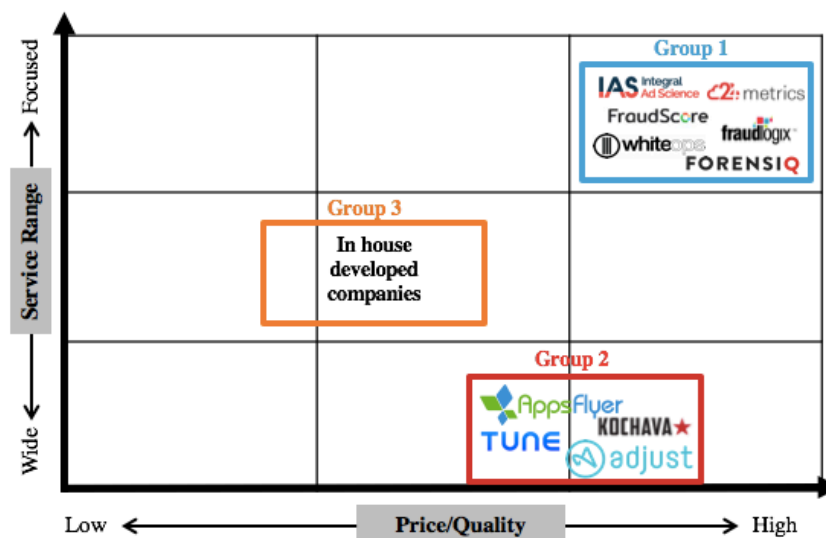
To sum up, we are facing an industry where suppliers, buyers, substitutes and new entrants are in a controlled power situation, despite the rivalry among existing firms being high. Through the analysis of the 5 forces of Porter it is possible to conclude that the mobile anti-fraud industry has an overall medium attractiveness – level 3 (mean). (See Annex XXII – 5 Forces of Porter – The Author, 2018).

8.2. Competition Analysis

8.2.1. Strategic Groups Analysis

In order to map the major strategic groups of the industry, two criteria were chosen – price/quality ratio and service range - as the core analysis dimensions. The competitors highlighted are those considered significant to the mobile ad fraud industry and whose strategies are similar.

Figure 5 – Strategic Group Analysis



Source: The Author, 2018

The figure above represents the three strategic groups that can be defined according to the service range offered – wide or focused – and their price/quality ratio.

Group 1:

Where the main players of the mobile ad industry belong due to their exclusive specialization in anti-fraud technologies. Inside this strategic group, one can find companies like Integral Ad

Science, ForensIQ, 24 metrics, FraudScore, WhiteOps and Fraudlogix. These companies sell their services to advertisers, publishers, agencies, and similar businesses.

By offering a specialized service, these companies are seen as having a unique know-how given that they invested solely in their technological preventive systems, have proven experience dealing with ad fraud, possess a wide range of clients and have gathered large data base of mobile devices from several regions. As such, these group of companies is perceived as having an overall very good price-quality ratio.

Group 2:

In this group, we can find other mobile ad support companies, such as mobile attribution and analytics ones - Appsflyer, Adjust, Kochava and Tune. These are big players in the market that have invested in brand extension strategies, creating add-ons to their standard attribution services. Appsflyer launched “Protect360”, Adjust has its “Fraud Prevention Suite”, Kochava created “Fraud Console” and Tune has its “Fraud Prevention Solution”.

As these companies have a fundamental role in the industry as attribution authorities – and it is essential to have an unbiased and independent attribution system –, they could capitalize from their good image amongst clients to sell their fraud prevention extension. However, the natural conflict of interest that emerges from trackers offering anti-fraud solutions as a paid solution could deviate potential buyers.

Group 3:

In this group are all the companies that are independent from third party tools and decided to invest internally by developing its own anti-fraud system. This way, they don’t depend from suppliers (Group 1 and Group 2). It is hard to identify these companies since not all disclose openly this kind of information.

Through this analysis, one can comprehend that there is a group of companies that developed ad fraud detection systems to help other companies to analyze their mobile advertising campaigns and eliminate bad quality and invalid traffic (Group 1). These are specialized enterprises in mobile ad fraud, that provide services to the other companies.

On the other hand, due to the growing market attractiveness, there are similar companies in the industry that have taken an interest in developing fraud protection solutions. It is the case of mobile attribution and analytics companies (Group 2) that, in addition to their main service, have designed extension features, that can be added on to the main package. Additionally, several companies have decided to develop their own tool, ceasing to depend from outsourced services, which allows them to reduce expenses (Group 3).

8.2.2. Industry Life Cycle

The mobile anti-fraud industry is going through a transition between growth and shake-out phase (See Annex XXIII – FraudProof Industry Life Cycle – The Author, 2018). Even though the industry is still developing, it has already a few key rivals in the competitive landscape.

Yet, with technology changing continuously and the current players still fighting for their market positions, it is considered an industry with growth potential and, as such, with room for more players to enter. That is why it is consider the industry to be evolving from stage 2 – *Growth* to stage 3 – *Shake-out*. When the rate of growth slows down and the demand approaches saturation levels – with the intensification of competition -, the industry will no longer be in transition but already in life cycle 3 – *Shake-out*.

8.2.3. Direct Competition

Now that the major competitors are identified, it is important to delve deep and exploit the particular characteristics of their business such as market share, positioning, strategies.

Three different groups were identified previously in strategic group analysis however, at this point, we will analyze only group 1, which is composed by the key anti-fraud experts in the mobile ad industry such as Integral Ad Science, WhiteOps, Fraudlogix, ForensIQ, 24metrics and FraudScore (See Table 4).

Table 4 – Major anti-fraud players (Group 1)

	Integral Ad Science	WhiteOps	Fraudlogix	ForensIQ	FraudScore	24metrics
Year	2009	2012	2010	2010	2016	2013
Country	USA	USA	USA	USA	Russia	Germany
N° of employees	500	>50	10-50	10-50	10	11-50
Revenue	>\$100M	N.D	N.D	N.D	N.D	N.D
Website	integralads.com	whiteops.com	fraudlogix.com	impact.com	fraudscore.mobi	24metrics.com
Major Clients	Facebook, Instagram, Youtube, Google, Appnexus, DataXu, Inmobi, Mopub, Yahoo	Adobe, The Trade Desk, Oath, TripleLift, Pubmatic, Appnexus, Playbuzz	YouAppi, Smart 3AdServer, AdsNative	Groupon, RocketFuel, Zillow, Yeahmobi, SmartyAds, Fetch, VertaMedia	Clicky, Headway, Curate Mobile, BoomMob, Cubic Games, Kimia, Rocket10	Bigpoooint Games, Affiliate Mob, Blind Ferret, Mozoo, European Games Group

Source: The Author (based on information available on companies' website), 2018

Integral Ad Science

With more than 500 employees and 22 offices spread around the 13 countries, Integral Ad Science (IAS) is one of the biggest measurement and analytics company in the advertising industry.

Founded in 2009, IAS works with more than 2500 publishers, 1600 advertisers, 150 programmatic partners. The growing partnerships, where Google, Facebook, YouTube are included -, allowed them to achieve in 2016 over \$100 million in annual revenue. Their solutions were recognized by Inc. 500, Crain's Fast 50, Forbes America's Most Promising Companies.

IAS has solutions specially designed for the intricate digital landscape, addressing therefore the different needs that brands, agencies, publishers and ad-tech companies have when it comes to the following three segments: ad-fraud, viewability and brand safety. There is no information available about pricing. Only upon request of more information the company will disclosure more details about pricing.

In June 2018, Vista Equity Partners acquired a majority stake in IAS in a reported \$850M deal. Scott Knoll, the CEO and President of IAS, revealed that intends to shift the IAS's expertise towards the old marketing channels like TV and billboard ads.

White Ops

White Ops is a cybersecurity company that provides online fraud detection solutions for digital advertisers, publishers and ad tech businesses. Over 5 funding rounds, White Ops has raised a total of 31 million dollars. White Ops's revenue has increased over 300% year-over-year during 2015. 700% growth in 2014. White Ops was ranked the 20th fastest growing technology company in north America on Deloitte's 2017 fast 500.

This company developed two products – “FraudSensor” and “MediaGuard”. MediaGuard is a predictive machine-learning algorithm that works alongside FraudSensor, a real-time bot detection system that aggregates a range of data points for each transaction registered. While FraudSensor detects fraudulent activity, MediaGuard is making sense of what was detected to predict the activity of bots. Pricing is not disclosed on the website. (See Annex XXIV – White Ops FraudSensor Summary Dashboard – White Ops, 2018; Annex XXV – White Ops FraudSensor Explore Dashboard – White Ops, 2018; Annex XXVI – White Ops FraudSensor Reports Dashboard – White Ops, 2018).

Fraudlogix

Fraudlogix is an ad anti-fraud company that provides solutions for networks, exchanges, SSPs & DSPs. The company highlights as their key features: “IP block List”, “Ad Verification Suite”, “Affiliate & Click Fraud Solutions” and “Threat Intel”. According to Fraudlogix, their machine learning technology allowed them to established ground rules when it comes to fraud, measuring effectively what is real and expected human behavior and what is considered an anomaly (traffic from bots, scripts, hijacked devices).

Its “Ad Verification Suite” is able to collect data from the user through a universal pixel, and report on several ends – ad fraud, viewability, brand safety and others. “IP Block List” is a technology that identifies and blocks traffic from bots, non-secure devices, malware, click farms, data centers, accessing the risk level of each IP. “The Affiliate & Click Fraud Solutions” allows partners to analyze the traffic in real-time (click and installs), identify and block fraudulent activity, and explore quality reports by source and sub-source level. (See Annex XXVII – Fraudlogix Affiliate Solution Dashboard – Fraud Report – ForensIQ, 2018; Annex XXVIII – Fraudlogix Affiliate Solution Dashboard – Analysis Reports – ForensIQ, 2018). “Threat Intel” is able to identify non-complaint devices in real-time within networks.

There is no information available about the pricings associated with the announced technology. Interested customers need to approach the company and schedule a call with a representative in order to get to know more details.

ForensIQ

ForensIQ is an anti-fraud platform that detects and blocks invalid traffic all across the funnel – from pre-bid programmatic buy to post-buy analysis – and on every device. ForensIQ was acquired by digital marketing platform Impact Radius for an undisclosed sum, after receiving a \$30 million funding round. Combined, the companies have about 275 employees and tackle different segments.

The company announces 4 different types of suites, that together give a 360 vision of the ad fraud: “ForensIQ Ad Verification Suite”, ForensIQ Firewall Suite”, “ForensIQ Install suite” and “Forensiq Performance Suite”. (See Annex XXIX – ForensIQ Ad Verification Solution Dashboard – ForensIQ, 2018).

ForensIQ’s ad verification solution is targeted for programmatic buy and analyses the post-bid of ad impressions, while ForensIQ firewall assesses the pre-bid, examining in real time if the traffic is legit. Additionally, ForensIQ performance suite analyses if the click, lead or conversion is suspicious, whereas the install suite checks if the installation of the mobile app or any event related with the install is considered fraudulent.

ForensIQ states that their technology is able to provide insights about the traffic quality provided by the suppliers, offering its partners with the necessary tools to improve traffic quality, whilst giving them detailed information (reasons and explanations), in case of a chargeback discussion.

FraudScore

FraudScore’s target are advertisers and ad networks. The anti-fraud service analyses the traffic coming from partners in order to find out fraudulent activity (conversion, install, registration, etc.) and empowers advertisers and ad networks to keep traffic clean – by rejecting proactively fraud conversions before communicating it to customer -, and improving reputation and relationships. According to FraudScore, it scored more than 300 000 000 conversions and checked more than 10 billion clicks.

Clients get a detailed report with the necessary data about the suspicious activity to show their partners. They score the traffic of each supply source on a scale of 0-100 (low index fraud to high index fraud). (See Annex XXX – FraudScore Dashboard – FraudScore, 2018).

Recently, FraudScore added a new fraud investigation solution – pre-bid technology –, which allows clients to analyze in real-time the amount of fraud per click and impression. (See Annex XXXI – FraudScore pre-bid dashboard – FraudScore, 2018)

FraudScore can be integrated directly with mobile tracking partners such as Adjust, Appsflyer, Tune, Optimob, Affise, Cake. The company offers several packages to meet the volumes of diverse clients, with pricing range from \$490 per month (with 30k conversions included) to \$1990 per month (with 250k conversions included). In the website, the pre-bid solution is not included in the packages previously mentioned, being considered an additional feature for clients. (See Annex XXXII – FraudScore Pricing Plans – FraudScore, 2018)

24metrics

24metrics is targeted for affiliates. Their tool – FraudShield – operates in real-time, being able to reject fraud once it is detected and to identify fraud behavior through the use of machine learning algorithms.

According to the company, FraudShield delivers solid reasons for rejecting fraudulent conversions whose evidences clients “can use in a court of law” (24metrics, 2018). This allows customers to grow margins by not paying for bad conversions and increasing payouts of the real ones. (See Annex XXXIII – 24metrics dashboard – 24metrics, 2018).

24metrics possess a comprehensive helpdesk available for everybody to explore, ranging from more tech related issues (like integration) to more practical ones (using the platform, billing, etc.). This shows that the company is focused on building a good customer experience. (See Annex XXXIV – 24metrics helpdesk – 24metrics, 2018). The company sponsors fast and easy “one click integration” with the most relevant trackers in the industry, and also its friendly pricing plans that are serve “from small businesses to corporations” (24metrics, 2018), starting from \$499 per month (30k conversions included) to \$1999 per month (250k conversions included). (See Annex XXXV – 24metrics Pricing Plans – 24metrics, 2018).

9. Internal Analysis

9.1. Brief contextualization of company

Mobrand is a mobile ad platform that offers a wide range of monetization solutions for CPI advertising. The Portuguese company was founded in 2015 by Luís Frade, Rui Mateus and Daniel Santos. Later on, the company was invested by OLAmobile, a marketing technology group based in Luxemburg that owns also other brands, such as Mobidea, Iconpeak, BidderPlace and EyeSee.

The Lisbon-based company closed 2017 fiscal year with a turnover superior to 5 million dollars and a profitable operation. The growth is the result of a small and young team of 10 people that aims to help the world's top app developers and mobile web publishers to achieve success on the growing marketplace.

Since the beginning Mobrand has been very focused on technology and creating the necessary tools to leverage the performance of their partners. The company believes automation and in-house developed tools are key to success since it throw-outs other companies' services.

Mobrand's first tool was Console, a platform where publishers can access the CPI campaigns, analyze in real time their performance and control their feed. Recently, in early 2018, Mobrand launched OfferTest, a system that allows CPI managers to make sure that their campaigns are redirecting correctly to the app store. The company had this technology available for internal curation purposes but decided to productize it as the industry still suffers with click waste and offer instability. OfferTest helps to identify all the companies involved in the redirection chain, making the app ecosystem more transparent and trustworthy.

9.2. Mobrand's Mission, Vision and Values

Mobrand's DNA is deeply connect with constant innovation and experiment, performance, and having team members capable of inspiring the collective genius. According to Mobrand (2017), the company's core mission, vision and values are demonstrated in the following statements:

Table 5 – Mobrand Vision, Mission and Values

Vision	“To bend, break and re-shape industries”
Mission	“To develop the technology that will become a standard on the client’s future”
Values	• Passionate about work • Critical thinking • Market focused • Delivering high performance while having fun

Source: Mobrand, 2017

9.3. Mobrand’s Portfolio Analysis

Mobrand’s self-serve publisher platform, **Console**, gives publishers direct access to a wide number of mobile campaigns, which they can monetize in a quick and easy manner. (See Annex XXXVI – Console, Mobrand's Publishing Platform – Mobrand, 2018). After their account is approved by Mobrand, publishers can choose from a variety of integration options – SDK, API, S2S -, and discuss the best option to monetize their traffic with their dedicated account manager.

The campaigns are automatically verified by OfferTest, and ranked by comparison with similar campaigns through what Mobrand calls “Demand Competition Generation Platform”. That technology ensures that only the best offers are open to publishers, excluding less competitive ones. Publishers can navigate through their analytics dashboard, where they can dig deeper into their overall apps performance (past or current) and also their traffic quality (valid or invalid clicks). There is also the possibility to export daily, weekly or monthly reports from the platform to better analyse the platform insights. Additionally, supply partners can use OfferTest inside the platform, having a limited number of tests per day. Publishers also have access to a skype smart bot, **Ted**, which provides useful information 24/7 in a few clicks, making the account management easier and automatic.

Advertisers don’t have a self-serve platform. Demand partners can either upload campaigns via API or manually. Nonetheless, they also have a dedicated account manager aimed to grow the account performance.

Mobrand's in-house developed **SDK** is connected with dozens of apps, delivering quality users and volume. It is available both on Apple's iOS and Google's android platform. Mobile app developers can easily integrate Mobrand's SDK into their app by adding a few lines of code and start to make money from advertisement.

The most recent product, **OfferTest**, is an offer curation tool that makes sure that the campaigns are correctly redirecting to the app store. (See Annex XXXVII – OfferTest – Mobrand, 2018). This product helps companies to avoid click waste and, subsequently, wastage of money. Additionally, marketers are able to identify all the companies involved in the redirection chain, which is an advantage for business development purposes. Users can test offers manually on OfferTest's website or on Console or bulk testing via API. OfferTest packages range from 50\$ to 2000\$, depending on the volume of tests (see Annex XXXVIII – OfferTest Pricing Packages – Mobrand, 2018). OfferTest is a pay as you go solution. As such, there is no monthly commitment associated. If users don't use the tests that month, they will continue to be available in the platform for the next months. All the packages include manual interface, API integration, customer and engineering support from Mobrand.

9.4. Project Presentation

The present project is a marketing plan for an anti-fraud solution, designed to protect mobile advertising companies from ad fraud, named FraudProof, that will be developed within Mobrand. This new product, that combines full funnel fraud detection, real time monitoring and optimization, behavior activity detection and prediction technology, materializes in an innovative, low-cost and easy to use SaaS platform. FraudProof has five different pricing packages available – 'Basic', 'Pro', 'Enterprise', 'Expert' and 'Custom' (per request only).

The use of tiered pricing based, popular in cloud companies, allows FraudProof to pursue different clients. In this case, price is linked to the clients' businesses volume size (number of conversions) and, also, the built-in features. For instance, the basic plan includes conversions analysis, however it limits the number of users and provides email only support. The expert plan, in its turn, includes not only conversions but click analysis – that is more complex –, has unlimited users, provides support via several channels (phone/skype/email) and includes employee training. Prices range from \$350 to \$2500 per month. The new business unit will share Mobrand's vision, mission and values mentioned previously as they accurately reflect FraudProof DNA.

10. Competitive Analysis (Internal and External)

10.1. Ansoff Matrix

Figure 6 – Ansoff Matrix

MARKETS	Current	Market Penetration Strategy	<u>Product Development Strategy</u>
	New	Market Development Strategy	Diversification Strategy
		Current	New
		PRODUCTS	

Source: Ansoff (1957), adapted from Lynch (2009)

Through Ansoff Matrix product-market strategy it is possible to conclude that the company will adopt a **Product Development Strategy** – it will try to increase its market share by offering a new product in the existing market. This can be accomplished through a more aggressive promotion and distribution as a strategy to find established customers in the market and also finding new ones. A thorough research should be conducted in order to map market and customers' needs.

10.2. SWOT Analysis

A SWOT analysis is a strategic technique that allows companies to assess the main factors that contribute to their business competitive position, emphasizing which ones can positively or negatively impact its goals. Mobrand's SWOT will take into account the company internal positive factors (strengths) and internal negative factors (weaknesses) as well as external positive factors (opportunities) and negative factors (threats). (See Annex XXXIX – SWOT Analysis – The Author, 2018).

Strengths

One of Mobrand's biggest strengths and what makes it really stand out from the ad networks crowd is the fact that it is not an ordinary ad network. Being proprietary of technology developed in-house brings an enormous competitive advantage to the business.

The recently commercially launched OfferTest, for instance, is a market success. This tool, that promotes the industry overall health by fighting click waste and offer instability, has added value to Mobrand's reputation in the industry.

The image of quality is also associated with the fact that Mobrand is listed as one stop shop for different kind of partners. In other words, Mobrand is able to work with everybody – from small app developers to big agencies and brands –, being able to deliver the highest possible ROI across all collaborations. Part of this strength is fulfilled by high quality traffic for advertisers and high quality campaigns for publishers.

Another big strength of Mobrand is its low-cost and adaptable structure component, when compared to other competitors in the industry. Its small team of 10 people cultivates a strong communication and information sharing element, which allows an internal prompt reaction to market changes. Moreover, the lack of bureaucracies helps to stimulate this high performance environment.

Likewise, the company disposes of high flexible operating costs since it uses external services for secondary activities, like hosting servers. Adding to these strengths, the business global scale also adds a positive note when it comes to sales.

Mobrand's role as a mediator and vast network connections on the industry and also established footprint of clients will allow a good jump-start for the anti-fraud solution. The company would leverage its client know-how to define a successful strategy.

Weaknesses

Mobrand's main business – as an ad network – is considered the most important weakness of the company when considering the development and launching of an anti-fraud solution.

Potential customers of the preventive platform may question the integrity and independency of the service. Since it would deal with large amounts of private data, Mobrand could leverage that information to its own interests as an ad network. One can argue that Mobrand could take advantage of it by letting bad traffic pass unscathed if it came from Mobrand sources or rejecting good traffic from partners that it wants to damage. As such, the double standard,

biased, lack of transparency and conflict of interest factors could represent a drawback in the future marketing and sales of the service.

To move forward with such project, the company would need to expand its workforce, since the current team is not enough to carry out a project of this size without further assistance. The project's initial investment would be average, depending on its ambitions. Furthermore, Finally, since the service would be hand out to other business, and that there is a fluctuating demand of mobile advertising driven by brand's budgets and periods, one can conclude that the product could also face the impacts of that oscillation.

Opportunities

The key opportunity is the growth of mobile ad fraud fueled by the users shift from traditional to digital media. With mobile becoming an increasingly important channel for businesses to have a relationship with their customers, the rise of mobile ad fraud has been duly noted by marketers. Having watched large sums of their budget disappear to fraud, companies are dedicating more efforts to fight it. The pressing need to tackle this threat, that is getting more and more sophisticated, is seen as the utmost opportunity for Mobrand.

Adding to that, the current and future generations are more technologically savvy than ever. Mobile phones are considered an indispensable object in millennials and Generation Z life's, being always within arm's reach. The growing market alongside the increasing number of smartphone users and their digital interaction through the use of apps make this a very appetizing industry.

The rapid technological change is also considered an opportunity as it could motivate innovative solutions, which in turn could potentially impact positively the performance, reduce costs and leverage the competitive advantage of the company.

Lastly, another opportunity identified is the increased popularity of cloud based services among small and medium companies, since it removes the need to invest in technology infrastructure, hardware or software licenses. Additionally, it allows companies to scale easier due to the its flexibility, customization, efficiency and overall low investment cost.

Threats

The constant evolving and changing market and its technology is one of the major threats to Mobrand's Business. The company and its team members need to think ahead to foresee major tech breakthroughs and market trends in order to not only keep up the rapid pace of change as stay ahead of competition. This, of course, demands and puts a lot of pressure on a small company such as Mobrand. However, given its structure, the overall communication, adaptation it is rather easier.

Digital ad anti-fraud market has been growing since more companies are advertising online. There are a few companies to cover this market necessity, which poses as a threat, especially in a B2B market, where the customers universe is potentially lower than a B2C market. Moreover, price wars with the competition is a likely situation, which could shrink the company's margin to a dangerous point.

Potential infringements lawsuits are also considered a possible threat as it is a common procedure in this industry to register technology related patents to avoid copy cats and losing market share.

As the digital advertising industry is still growing, it is safe to say that there are not a lot of specialized professionals in this area, and the net it's getting tighter if we talk about mobile ad fraud. Failing to find the necessary workforce in Portugal, where Mobrand is based, the company would have to contract resources without knowledge and invest effort, money and time in training.

Finally, one needs to stress the importance of privacy and security since the company deals with a very valuable asset: user data. Additionally, any change in regulation and laws can potentially distress the business.

Each of the SWOT analysis factors will be defined according to its relevance, attractiveness or impact: from 0 (no relevance/attractiveness/impact) to 5 (extreme relevance/attractiveness/impact). While external factors will be defined according to its attractiveness (Opportunities) and impact (Threats), internal factors, like strengths and weaknesses will be defined according to its relevance. Additionally, each factor will be assessed according to its future evolution: increase, decrease or stability (See Table 6 and 7).

Table 6 – Hierarchical SWOT: Internal Analysis

Internal Analysis		
Strengths	Relevance	Evolution Forecast
Proprietary technology developed in house	5	Increase
One stop shop for different kind of partners	5	Increase
High quality traffic and high quality campaigns	4	Increase
Low cost structure compared to other companies in the industry	4	Decrease
Flexible operating costs	4	Stability
Existent Mobrand connections with major players in the industry	4	Increase
Boundary less	3	Stability
Weaknesses	Relevance	Evolution Forecast
Mobrand's ad network image	5	Stability
Medium initial investment	4	Stability
Low time and HR resources availability to develop new projects	3	Increase
Fluctuating demand for mobile advertising products/services	4	Increase

Source: The Author, 2018

Table 7 – Hierarchical SWOT: External Analysis

External Analysis		
Opportunities	Attractiveness	Evolution Forecast
Growth of mobile ad fraud	5	Increase
Growth of mobile advertising eco-system	5	Increase
Current and future generation are technologically savvy	5	Increase
Rapid technological change which motivates innovative solutions	4	Increase
Increased popularity of cloud based services	4	Increase
Threats	Impact	Evolution Forecast
Rapid technological change	5	Increase
Significant global competition that offers similar services	4	Increase
Price wars with other players	4	Stability
Patent infringement/ Potential lawsuits	5	Increase
Few specialized workforce in mobile ad fraud in Portugal	4	Increase
Privacy concerns and security risk	4	Increase
Changes in environment, law and regulations	4	Increase

Source: The Author, 2018

11. Survey Analysis

A survey was conducted to better understand marketers' point of view on the current and estimated state of mobile ad fraud, and to evaluate the pertinence of a new SaaS anti-fraud solution for the mobile industry. Taking into account global scope of this industry, the questionnaire was published online during the month of September of 2018, and distributed to marketers via email, Skype and LinkedIn, obtaining answers from 100 respondents. (Annex XL – Mobile Ad Fraud Survey – Survey, 2018). The main purpose of this online survey was:

- To perceive the main characteristics of marketers and their companies.
- To understand marketers' point of view on the state of mobile ad fraud.
- To understand marketers' actions and priorities to combat mobile ad fraud.
- To evaluate the pertinence of a new SaaS ad fraud preventive solution.
- To find out about the top-of-mind characteristics for marketers of a potential new anti-fraud solution.

The first five questions were broad-spectrum and aimed to characterize the respondents company background such as their role in the industry, preferred pricing model to acquire paid users, size and location of the organization.

The great majority of respondents (97%) works in the mobile ad industry, against 3% that work in similar industries. More than half (52%) said to work for Ad Networks, 19% for Agencies, 14% for Advertisers and 7% for Publishers. Amongst the favourite pricing model of the respondents is cost per install (78%), followed by cost per action (16%). A small portion selected other options available like cost per click (3%), mixed models (2%) and cost per thousand impressions (1%). Concerning the size of the company they work for, almost half of the respondents (47%) said that their company has between 1-50 employees, 33% between 51-200 employees and 12% between 201-500 employees. A small number of respondents said to belong to organizations with a size between 501-1000 employees (2%) and superior to 1001 employees (6%). Almost half of the respondents came from Asia countries (49%), with Europe countries representing 38% of responses, North America following with 10% of responses and South America representing only 3%. (See Annex XLI – Questionnaire Responses by continents location – Survey, 2018).

11.1. Questions related with key industry challenges and mobile ad fraud

The first question non-related with respondents' characterization required marketers to rate, on a scale of 0 to 5, the importance of some of industry biggest challenges like privacy, ad fraud, attribution, brand safety, and others. Amongst all the other options, "Ad fraud" was considered by 76% of respondents to be "extremely important", followed by "User Quality" (45%) and "Transparency and Trust" (42%).

The survey intended also to grasp how concerned are marketers when it comes to ad fraud on mobile devices. The results revealed that 83% are "very concerned", 15% "somewhat concerned", with only 2% of marketers stating to be "not concerned". (See Annex XLII – "Overall, how concerned are you about ad fraud on mobile devices?" – Survey, 2018).

When questioned about the likelihood of mobile ad fraud to increase in 2019, a big slice rated as "very likely" (38%), "likely" (28%) and "extremely likely" (21%). Only 2% of marketers considered it to be "Not likely at all". (See Annex XLIII – "On a scale from 0-5, how would you rate the likelihood of mobile ad fraud increase in 2019? (0 being not likely at all and 5 being extremely likely)" – Survey, 2018).

11.2. Questions related with internal decisions regarding mobile ad fraud

When addressing decisions made inside their organization, mobile app marketers answers disclosed that their companies take ad fraud as a serious problem and are taking several actions to prevent it. 58% of respondents classified the priority given by their companies to mobile ad fraud prevention as "extremely high" and 30% as "very high".

The next question wanted to understand if companies are contracting external anti-fraud tools. In this case, 66% of marketers revealed that their company uses a third party tool, against 34% that does not contract any service. Still, even with overall industry taking measures to tackle fraud, marketers acknowledge that sizeable portion of their mobile ad budgets are lost to fraud. For instance, 35% of respondents estimate to lose between 20%-29% of their mobile ad budget to fraud, while 29% disclose to lose less than 20% and 20% between 30-39% of their budget. A minority (16%) believes to lose more than 40% of its overall budget. (See Annex XLIV– "How much of your mobile ad budget do you estimate is lost to fraud?" – Survey, 2018).

The survey wanted to comprehend likewise the three most visible actions that marketers identify as has been taken currently by their companies to tackle fraud. In this matter, over 80% of respondents selected “We analyze data to detect fraudulent patterns”, followed by “We developed internal measurement and detection tools” (69%) and “We implemented a blacklist service” (48%). A minority cite to not have plans to take any action (3%), while others say to have not taken any action but plan to do so (3%).

As expectations of fraud budget to change next year, 65% of players of the mobile advertising landscape believe that their company will increase the budget dedicated to fraud prevention in 2019. However, 15% expect no change in that area, while 14% answered not knowing. (See Annex XLV – “How do you expect your company dedicated fraud prevention budget to change in 2019?” – Survey, 2018).

Taking into account the marketers’ awareness of mobile ad fraud growth, some questions were made to perceive if the industry has enough knowledge about fraud as well if they understand the solutions available. Data shows that more than 80% of marketers agree that today’s fraud evolves too quickly, being hard for organizations to keep up the pace. Even though marketers recognize the current challenge, 53% of respondents disagree to have lack knowledge about the existing types of mobile advertising fraud to successfully tackle fraud schemes. Furthermore, marketers cite to have understanding about the existing solutions that fight mobile fraud and to have the necessary technology to detect, monitor and prevent it on a daily basis.

11.3. Questions related with the launching of a SaaS anti-fraud solution

In this set of questions, marketers were asked to contemplate the hypothetical creation and launching of an anti-fraud platform, that would be designed from scratch, and furthermore address the most critical set of features that the service would have to provide. Marketers considered the following aspects to be **extremely important** when designing a new service:

- **Full funnel fraud detection – from click to install** – Almost 60% of marketers believe that the ability to analyse the entire chain, from click to install (or even post-install events), is fundamental.
- **Real-time monitoring and optimization** – The evolution of fraud techniques created a sense of urgency in the industry. For that reason, 58% of marketers believe that real-

time detecting and blocking is necessary to avoid further damages. However, it could fail to identify more advanced fraud forms and patterns.

- **Behaviour activity detection technology (human or bot)** – More than half of the respondents (53%) considers that the anti-fraud should be able to detect non-human traffic through behaviour pattern.
- **Live alerts** – 42% marketers want to be warned when major fraudulent activity is happening in order to maintain a certain level quality, avoid damaging relations with partners.
- **Big data analytics** – A comprehensive analysis of traffic from sources and sub sources and other relevant data is thought to be important by 42% respondents.
- **Predictive machine-learning algorithm** – 40% of marketers consider that, besides detection, the new solution needs to possess latest technology in machine learning in order to predict the presence of fraudulent activity, like bots. To achieve that, a deep data analysis of data is required to discover and comprehend fraud patterns.

To understand the most important factors marketers consider before purchasing an ad fraud detection solution, respondents were asked to select the top-of-mind factors that would influence their buying decision. The survey divulged that the factors that would most impact the sales would be:

- **Product Quality** - 74% of marketers cite that overall product quality is the most important criteria.
- **Integration with trackers and marketing platforms (41%) and Compatibility with current infrastructure (38%)** – Marketers demonstrate to have tech concerns when they are planning to purchase a new service. This indicates that a new service must have an infrastructure that can be effortlessly integrated with a wide range of partners, or with in between services like trackers.
- **Ease of use (32%)** – Fraud is a complex concept to understand. Therefore, the design will have a key role in displaying all the information in a simple and attractive way that promotes equally functionality and ease of use.
- **Innovative features (29%)** – Respondents consider that a potential new solution should have an original factor in order to stand out from the other competitors.
- **Price (28%)** – Marketers also perceive price as a success factor that has a direct effect on business success.

12. Project SMART Objectives

To define the project strategic objectives, a strategy management framework will be implemented - balanced scorecard (BSC). BSC tool allows to map high-level goals of a company by analysing four perspectives: Financial, Customer, Internal and Learning & Growth.

Table 8 – FraudProof Objectives

Area	Objectives
Financial	• Break-even should be achieved before two years of activity. • Complete the first year of activity with, at least, 150 customers. • Achieve high profitability per employee.
Customer	• Achieve a referral rate of 5% by the end of the first year (for every 100 new users, 5 must be by customer referral) and 10% by the end of the second year (for every 100 new users, 10 must be by customer referral). • Achieve a free trial conversion rate between 10-20%. • Provide best product value for price, meeting and exceed customer expectations – creating strong relationships and building brand identify. • Understand the customer needs and wants, maximizing the lifetime value (retaining the customer). • Provide good customer support experience. • Ensure a monthly churn rate (existing customers that cancelled the service) below 5% in the first year (for every 100 new clients, the company losses 5) and 3% in the second year and less in the following. • Develop a customer satisfaction survey every 6 months to evaluate the platform's function and collect feedback from new released tools.
Internal	• Monthly brainstorming meeting, where each team member must show up with a timely and executable feature for the platform. • Ensure the availability of at least one employee to support actively customer support service. • Ensure that FraudProof's blog and social media pages are updated regularly (minimum one week publication). • Create a high-achievement environment. • Implementation of a system of professional evaluation of employees (to be done after the first year of company activity).
Learning and growth	• Leverage technology to improve platform efficiency. • Invest in research and development.

Source: Author, 2018

13. Development Strategy

13.1. Strategic Approach

In 1980, Michael Porter defined three generic strategies that a company can pursue when choosing the type of competitive advantage – lower cost, differentiation or focus –, and the market scope – broad or wide. The anti-fraud SaaS solution intends to penetrate the market using a cost leadership strategic approach, by implementing lower prices than the competition, without compromising the quality (See Annex XLVI – Michael Porter Generic Strategies – Michael Porter, 1985). The choice of a low cost price strategy takes into account the potential scale effect. Having a lower pricing points allows FraudProof to access a large number of data points from various companies in the industry, to develop more knowledge about ad fraud and to improve the product during the course of these innovations. In the future, with a reasonably better product, it will also be possible to follow a up market movement. In order to achieve such strategy in a sustainable way, the company will develop the tool internally since it will be an important asset for the company. In that sense, we avoid outsourcing and being dependent of others. For that, high levels of efficiency are required when developing the SaaS product. Moreover, cost and quality control will need to be tightly monitored in order to achieve a good balance in what concerns quality-price ratio.

13.2. Segmentation

To correctly address potential customers and define a relevant positioning, it is vital to comprehend what type of customers will the SaaS product attract. In order to achieve that, it is necessary to segment the market, since each customer/business has potentially unique needs and desires. One of the most common approaches in B2B markets is to follow a market segmentation based on business customer demographics. Alongside behaviour, these two segmentation criteria are considered to be the most adequate, when considering the project's final goals and survey's results.

Taking into account that the CPI market does not possess a large structure and B2B intrinsic characteristics, the author considers that anti-fraud solution should offer different solutions, tackling the singular needs of existent companies available – a strategy that is already being followed by main rivals. In that sense, the pricing packages will have in mind the volume of

activity of the company¹ and, as such, its size. The table underneath describes respectively each of the variables chosen, which allows a more efficient segmentation of the target market.

Table 9 - FraudProof segmentation criteria

Criteria	Variable	Target
Demographics	Industry	CPI mobile ad companies
	Company size	Small size companies Medium size companies Big size companies
Behavioural	Usage Rate	Light users Medium users Heavy users
	Purchasing function organisations	Focus on decentralised purchasing companies
	Nature of existing relationships	Primary focus on companies with whom there is already a strong relationship

Source: The Author, 2018

13.3. Target

The target-market that the SaaS product will pursue are worldwide small, medium and big size CPI mobile companies. This is based on the questionnaire results that highlighted not only the wide geographical scope as the wide-ranging company size. Besides that, we will only pursue companies whose revenue model is cost-per-install – the preferred model by 78% of the marketers, according to the survey. That said, it is not uncommon that companies that work with more than diverse revenue model (CPC or CPA) could become a future target.

The product's primary focus will be on companies with whom there is already a strong partnership, leveraging Mobrand's existing contacts, which provides a competitive advantage. Efforts will also be done to identify decentralised purchasing decision companies since this will shorten the customer conversion time.

13.4. Positioning

Product positioning is considered crucial during the buying process. Thus, it is a vital opportunity that the company should not disregard, on the contrary, it must be contemplated in way that creates a spot-on perception and image of the product in the target-market mind's.

¹ By volume, we understand the number of conversions that will be analyzed by the solution.

Table 10 describes with more detail the segmentation that is taking into account when looking specifically for the variables industry, company size and usage rate.

Table 10 - Detailed FraudProof segmentation criteria

Company size	Usage Rate	Volume Size	Positioning
Small size company	Light user	30,000 conversions	The service will be designed for small brands, with small technological and people infrastructure. It will limit the number of users with access to the platform. Given the reduced price, customer support options will be reduced.
Medium Size Company	Medium user	100,000 conversions	The service will be designed for growing brands, with small to medium technological and people infrastructure. It will have unlimited number of users with access to the platform. Besides that, more customer support options will be available as well as employee training.
Big Size company	Heavy user	250,000 conversions	The service will be designed for established and big brands, with medium to high technological and people infrastructure.
		22 billion clicks/425,000 conversions	For this segment, three different solutions will be offered, depending on the type of conversions to be analysed.
			Likewise, it will have unlimited number of users with access to the platform. Besides that, more customer support options will be available as well as employee training.
		Tailored service (Any volume)	Option 2 will add a new feature – click analysis. Since the click analysis is more complex, this will raise the price but still be consistent with the survey analysis that required a full funnel fraud detection. Option 3 will leave the door open for big businesses that don't see any of the other two options fit into their current needs and wants.

Source: The Author, 2018

13.4.1. Golden Triangle of positioning

Lindon *et al.* (2014) defined three factors that validate the positioning: consumers' expectations, competitive positioning and potential trumps of the service. Together, these elements create what the authors named the golden triangle of positioning. FraudProof's potential consumers expect to have a good quality, innovative and easy-to-use anti-fraud solution. Taking into account the competitors impartial and specialized positioning, the product will stand out due to its price quality ratio, transparency and overall value positioning (See Annex XLVII - Golden Triangle of Positioning of FraudProof – The Author, 2018).

Consumer's Expectations

Marketers expect a SaaS solution that provides a good quality, innovative features (full funnel fraud detection, for example) and a smooth, easy-to-use technological interface that is able to

connect easily with their company's infrastructure. This set of expected characteristics were identified in the survey previously developed.

Competitive Positioning

The most direct competitors of FraudProof are projects that dedicated their attention solely to fraud investigation and to the development of technologies and tools to prevent it, and do not possess further businesses related with the advertising industry. Therefore, their concept is associated with impartiality and specialization.

Potential Trumps of the Service

FraudProof will offer different solutions for different target-market. That said, one of project's main trump will be directly correlated with its value positioning. Depending on the pricing solution, FraudProof will use a 'more for less' positioning – by introducing a product with comparable quality with other competitors however at a lower price –, or 'the same for less' positioning.

Moreover, FraudProof will be completely transparent about how their technology detects and blocks fraudulent activity, and their pricing packages. When searching for a new anti-fraud solution, potential customers will find in FraudProof website the necessary data and clarifications to proceed, if they want, in that same day with the purchase - creating a smooth user-friendly flow, always backed up with the necessary customer service.

Another potential trump of the service is the fact that, as the survey exposed, marketers are very concerned with mobile ad fraud, are increasing their budgets to prevent it and believe that mobile ad fraud will continue to grow in the next year.

13.4.2. Perceptual map

The perceptual map is a tool that positions a brand in relation to other competitors in the market. The following perceptual map is based on the results obtained from the questionnaire that was conducted, which lead to the definition of the most important benefits in consumer purchase decision, and is in line with the competition analysis previously developed.

The two most important characteristics pointed out by marketers as having influence in the decision-making at the purchase moment are: “full funnel fraud detection” and “real time

monitoring and optimization”. (See Annex XLVIII – Perceptual Map of FraudProof – The Author, 2018).

The horizontal axis describes the real-time monitoring and optimisation – whether it is good or poor. The vertical axis describes the full funnel fraud detection– whether it is complete or partial. As shown, the most significant competitors for FraudProof are those who provide a complete full funnel fraud detection and provide a good real time monitoring and optimization service.

Taking into account these two characteristics, 24metrics and FraudScore positioning as having a good real time monitoring and optimisation feature but having a partial full funnel fraud detection, whereas Integral Ad Science, ForensIQ, Fraudlogix and WhiteOps are perceive to have a complete full funnel fraud detection and a good real time monitoring and optimisation capabilities.

FraudProof’s positioning is in the segment of services that provides a complete full funnel fraud detection and offers a good real time monitoring and optimization. This positioning considers the fact that FraudProof will offer different kind of solutions, therefore attracting a wide range of customers, with distinctive needs and requirements.

14. Critical Success Factors

The following elements are crucial for the company to succeed in this market, not only internally but also externally:

To have an innovative and quality product – Given the continuous technological change and the growth of mobile ad fraud, it is vital to keep up with the newest developments, cultivate a deep understanding of the mobile ad fraud and to have the standards aligned with the reality in order to provide a secure and constantly-evolving detection product for companies.

To be an easy to use and intuitive product – Fraudsters are sophisticated, as such, the product must also be sophisticated. However, it should provide a good user experience – easy to navigate and maneuver.

To be affordable and price-competitive – To develop a low-cost solution to fight the already established companies in the industry, providing friendly pricing approaches to the customers.

To connect in a fast and seamless way with the current infrastructure of potential partners and integrate easily with trackers/marketing partners – To avoid losing prospects, the solution should be easy to integrate in any platform and 3rd party systems (trackers, for example). Custom integration should not be an obstacle.

To have a high performance and scalability technological infrastructure – The platform needs to be agile and responsive while providing a good user navigation and secure experience.

To develop a marketing strategy focused on leverage customer experience and user conversion into clients – Engage with users in an individual and personalized way to promote a seamless conversion and, later on, a satisfying customer experience that stimulates referrals.

15. Implementation Policy Definition

15.1. Marketing-Mix

15.1.1. Product

FraudProof is an anti-fraud SaaS solution designed to help mobile marketers to fight mobile ad fraud. It detects fraudulent activity in real time, protecting companies from one of the pressing problems within the industry. To guarantee brand's rights, FraudProof will be registered in Instituto Nacional da Propriedade Industrial (INPI).

Name

When brainstorming about the name for the product, the author wanted a catchy sound that created an immediate image in the customers head and, at the same time, communicate consumers its core mission – fight mobile ad fraud. The name “FraudProof” is a combination of “Fraud” and “Proof”, which means that is designed to resist the impact of fraud, that is impenetrable to fraud.

The name was inspired by outdoor clothing companies. Their products often advertise waterproof, windproof, coldproof technologies, and are built for explorers who are exposed to extreme weather conditions and need to stay warm, dry, comfortable and secure. The main goal of those products is to enhance protection and allow better body function – improving overall performance and endurance.

Similarly, marketers are also facing adverse conditions in mobile ad landscape and need to protect themselves from fraud by implementing a quality and trustworthy fraud detection solution. “FraudProof” aims to protect the explorers of the mobile ad ecosystem by providing an effective detection solutions that fights cybercriminal activity.

Colour Scheme

Colours are strategic in graphic design, since it can stimulate a certain mood or transmit a determined message, increasing the effectiveness and recognition of the brand alongside customers. Thus, it is important to think wisely about what kind of subconscious judgment we want customers to have when looking at FraudProof logo design.

Technology brands are known to use the colour blue since it conveys feelings of trust, credibility, security, professionalism and reliability. Dell and IBM take advantage of this colour, for example. Another option would be to use black and white given the duality of sensations it provides. White is associated with purity, safety, integrity while black is often considered to be the colour of power, sophistication, strength, accuracy. Paired together, black and white can create a strong marketing impact. Companies like Apple and Sony choose this combo. FraudProof wishes to transmit safety, sophistication, professionalism, liability. The design will have black and white with an emphasis colour (blue) to draw people's attention.

Logotype

The brand logo is composed by the project's name – FraudProof -, and a symbol. Companies that deal with security and fraudulent activity normally use an image or symbol in their logo. Amongst common images are shields, key, locks, fingerprints, fraudsters silhouette, magnifying glass, for example. FraudProof logo will have a key lock inside a search icon. (See Annex XLIX – Official logos of FraudProof – The Author, 2018).

Website

Taking into account that all activity happens exclusively online, the website is of pivotal importance – it needs to be accessible, search-engine optimised, have coherent content and an overall aesthetic look (See Annex L – Future FraudProof Website (Landing Page) – The Author, 2018). Those features are crucial to encourage visitors get to know better the product. FraudProof website will respect the following structure:

- Landing Page with 'call-to-action' (CTA) buttons along the page
- Product (How does it works, main features)
- Pricing (Pricing options available, with comparison tool)
- Blog (Videos, Articles, etc.)
- About (Company, Team, Tech Partners, Location, Contacts)
- Log In/Register

The website will be built in a way that motivates visitor conversion with several CTA buttons, strategically positioned along the pages. For example, a CTA button that encourages visitors to start a 30-day free trial with no strings attached, subscribe email newsletters, follow social media channel, download case studies, amongst others. Besides, to provide a great customer experience, a 24/7 live chat service will be contracted to support any potential leads and

motivate user conversion. When a team member is not available to answer, a chat bot will engage with visitors, sending automated messages and replying to frequently asked questions (FAQ).

The Anti-Fraud Technology

FraudProof will take into account the insights of the survey into the architecture of the product. Marketers were asked to describe the set of features they would most appreciate in such tool, if they could create one from scratch. Table 11 describes the set of characteristics that the anti-fraud solution will possess.

Table 11 – Technological architecture of FraudProof

Feature	Description
Full funnel mobile fraud detection	FraudProof will provide a pre-bid and post bid analysis API solution. This means that it can analyze whether a click or conversion of a mobile app is fraudulent in real-time.
Real time monitoring and optimization	The solution will not only identify but also block malicious activity. Customers will always have a final say, deciding if they want to let it pass through, for example.
Behavior activity detection and prediction technology & big data analysis	Machine learning algorithms that are able to recognize hidden fraud patterns and behaviors, thus being able predict and detect bot activity.
Easy integration	Customers can choose to add S2S postback, integrate FraudProof API or integrate directly with the mobile tracking or marketing partners they are already using.
Reporting Dashboard & Extensive Reports	Comprehensive dashboard to help marketers to quickly and easily analyze fraudulent activity. Possibility to export the desired data into csv, xls or pdf reports.
Live Alerts	Customers will be notified via email or other channel when malicious sources are identified.
Custom API parameters	Clients will be able to configure their accounts, being able to define, for example, minimum/maximum thresholds.
High Security System and Single Sign-On	The client's information will be properly secured. The platform will also have a login authentication mechanism that allows users to access with one single identity.

Source: The Author, 2018

Annex L explains in a synthetic way the information flow of the anti-fraud solution. In other words, how FraudProof operates and communicates with its partner the quality results it obtained from the analysed installs. (See Annex LI – Information Flow of the FraudProof – The Author, 2018).

The Platform

Customers should navigate easily in the platform that will prioritise functionality, usability and design. Given the complexity of fraud, design is considered a key factor for the success of the product. The platform needs to display information in a simple and engaging way, capturing the consumer attention from the first look. The interaction between the platform and customers should be as smooth as possible in case any doubt arises. Customers will have an array of possibilities to reach customer support team – email, phone, skype -, depending on the type of package bought.

The platform will have the following sections: Dashboard, Reports, Integration, Profile and Help. The initial dashboard will allow customers to check quickly the fraud summary, fraud profile and their estimated savings. In the reports section, they are able to customize their reports, choose the data looked-for, being able to export them into csv, xls or pdf files.

In the integration section, clients will find a simple explanation of how to integrate FraudProof. In profile section, customers are able to add new users, add billing information, purchase another package, see how much of the current package they have already spent. In help, a wide range of articles will be available with FAQ, divided by themes – “Getting started”, “Integration”, “Reporting”, “Billing”, “Video Tutorials”, “Troubleshooting”.

The most important sections of the platform would be the dashboard and reports, where the foremost information would be displayed. For example, in ‘Fraud Summary’, users would be able to check the most recent metrics in what concerned fraudulent activity. The data will be presented in customizable interactive charts. The key information available would be: total conversions, total rejections, % of rejected conversions, % of approved conversions, rejected conversions overtime, summary of most fraudulent activity (per campaigns, bundleIDs, countries, source, publisher).

Taking into account the analysis, users have the option of blocking on the spot sources or publishers. They can also review the account blacklists status at any time (adding/removing blacklists), having complete power to manage the actions made either done in real-time by the platform or by the user itself. (See Annex LII – Blacklist option – The Author, 2018).

In ‘Fraud Profile’, users would be able to breakdown information by campaign, identifier, publisher, source, and analyse the overall quality of the traffic received. Here are some of the key data that would be available:

- Number of invalid traffic coming from bots, data centers or compromised devices
- IP Addresses with high click/conversion volume
- Devices with high click/conversion volume
- Click-to-Install Rate (abnormally fast or low installs)
- Rebrokering

To help marketers measure the effectiveness of campaigns, FraudProof will provide reports. To get an overall view of the performance, users can check the Fraud Report. The report is customizable, which means users can add/remove columns. (See Annex LIII – Reporting option – The Author, 2018).

Overall, FraudProof dashboard will aggregate more than 100 data points: identifier, campaign ID, publisher ID, source ID, number of clicks, number of unique clicks, number of installs, number of unique installs, conversion rate, Session IP, % duplicated IP (clicks and conversions), click time and install time, click to install time (seconds), Country, Device Language, % of Device language/Country mismatch, Browser, User Agent, Device Brand, Device Model, Device Operating System Version, Device ID, Mobile Carrier, Traffic App Origin, IDFA, GAID, In-App Events, Revenue.

In the platform, users will be able to access their “Estimate Savings”, where they can see how much money is FraudProof taking from fraudsters hands. The data is calculated on a daily basis and can be filtered by “App Name”, “Source”, “Publisher”, “Geo”. The results of that research can also be exported in CSV reports. (See Annex LIV – Estimated Savings Option – The Author, 2018).

The packages

Customers will have the possibility to choose between multiple packages, with different combinations of volume and features at diverse price points. Each tier is tailored around the needs and budget of a type of potential customer. Accordingly, FraudProof will use a tiered based pricing, which is the most common model in SaaS companies (See Table 12). The price will be directly associated with the volume size of the company – conversion wise –, and the needed functionalities (See Table 13).

Table 12 - FraudProof packages

BASIC	PRO	ENTREPRISE	EXPERT	CUSTOM
<i>For Small Brands</i>	<i>For Growing Brands</i>	<i>For Established Brands</i>	<i>For Big Brands</i>	
Limited Users only	Unlimited Users	Unlimited users	Unlimited users	
30,000 conversions analysis	100,000 conversions analysis	250,000 conversions analysis	22 billion clicks analysis	
Email support	Skype/ Email Support	Phone/Skype/Email Support	425,000 conversions analysis	Any volume
	Account Manager	Dedicated Account Manager	Phone/Skype/Email Support	Any platform
	Employee Training (2h)	Employee Training (2h)	Dedicated Account Manager	Custom features
			Employee Training (3h)	

Source: The Author, 2018

The ‘Basic’ package, for instance, is targeted for small structure brands, with low volume analysis need. As such, these clients will have a limit number of users with access to the platform and email support only. As we move to the following option, we increase the volume of conversion analysis as well the number of features included. For example, the next package – ‘Pro’ –, is designed for growing brands. Thus, it includes an unlimited number of users with access to FraudProof, email and skype support, an account manager and also 2h of employee training.

The option with more functionalities included, and therefore the most expensive one, is ‘Expert’, which was designed for big brands, with high volume analysis demand. This is the only package that includes click analysis, a more complex element that companies with higher marketing budgets seek for in anti-fraud solutions. It includes all the functionalities of the

previous packages and more: a dedicated account manager plus one more hour of employee training.

The last package – ‘Custom’ –, was created to avoid losing clients that did not find what they were looking for in any of the previous packages, either due to volume size or set of features. This option allows a total customization of services and, therefore, its value will depend on what the customer needs.

Additionally, FraudProof will offer free trials for each pricing plan available, as that will allow potential customers to get to know the product first-hand. The free trials will have a duration of 30 days.

15.1.2. Price

Setting a price is a big challenge for an online business since internet gives the opportunity to compare to similar products and prices in just a few clicks. FraudProof will follow a **penetration strategy**, which means it will offer a low cost solution. In that logic, the platform expects to attract existing and prospective customers more easily. FraudProof package prices range from \$350 (‘Basic’) to \$2500 (‘Expert’) (See Table 13).

The platform will be fully transparent regarding the pricing information in order to avoid discomfort, promoting a ‘no surprises and hidden costs’ policy. If customers reach their monthly volume before the date, they can determine if they accept FraudProof to charge for extra conversions, and continue to be protected, or if they prefer to buy another package instead. In the second scenario, customers are warned automatically via email when they are reaching capacity. If not sure which solution provides the best fit to their company, costumers are also able to access a comparison tool or contact sales representative via email or skype.

Table 13 – FraudProof pricing packages

BASIC	PRO	ENTREPRISE	EXPERT
\$350 per month +\$0.02 extra conversion	750\$ per month +\$0.01 extra conversion	\$1550 per month +\$0.009 extra conversion	\$2500 per month +\$0.007 extra conversion
Price per conversion: \$0.011	Price per conversion: \$0.0075	Price per conversion: \$0.0062	Price per conversion: \$0.0058

Source: The Author, 2018

Comparing to the companies that have, to our best knowledge, the lowest market price, FraudProof will practise the most aggressive price-point (See Annex LV – Pricing comparison with competitors – The Author, 2018).

Paralleled with 24metrics, customers would have the exact same conversion volume while saving up to \$140 in the first tier, \$249 in the second tier and \$449 in the third tier. FraudScore has a more aggressive approach to price than 24metrics. Nevertheless, FraudProof customers would save \$40 per tier. The big difference here is in the 4th tier package, in which FraudProof will offer a full funnel analysis – from click to conversion. Neither FraudScore and 24metrics offer click analysis, so this will be a differentiated service.

15.1.3. Placement

There are two important channels to be considered in FraudProof placement. Both will serve different purposes. One channel – **engagement channel** -, will allow potential clients to reach out and get to know the value proposition of FraudProof through a digital medium, like social media (Facebook, Twitter, LinkedIn), search ads and display ads. These channels will drive the potential client to FraudProof website. Reaching this level, the user will be able to have its first contact with the product, evaluate its value proposition, register to use the 30-day free trial or buy its first package, thus becoming a client.

FraudProof website is considered to be the **deliver channel**, since it is the main window to raise consumer awareness, engage and convert leads into clients. Customers will be able to access it at any time, any place through desktop, tablet or mobile. Besides that, as customer experience is key in a cloud-based services, clients will have several points of contacting Fraudproof:

- 24/7 Live chat system – customers can talk directly to FraudProof's team, if available, or be assisted by a bot that will engage and answer FAQ. Each conversation is being reported in real-time to FraudProof. Any unsolved issue will be sent to Fraud Proof's team.
- Email and Skype support.

To have a high performance business, it will be important to have a discoverability strategy defined to showcase the website at the right time for the right audience. Again, search engine optimisation will be critical to have a good rank when potential customers are searching for anti-fraud solutions on the internet.

15.1.4. Promotion

Taking into account that this is a digital only project, its promotion and communication strategies will also be digital. Thus, the platform will interact and engage with prospects and customers through digital strategies, actions and tools.

FraudProof will invest time in creating relevant and valuable customer content that will feed not only the Website Blog but several social media pages. Fraud Proof will be present on LinkedIn, Twitter and Facebook.

These platforms will be useful to create brand awareness and promote the brand itself, reaching existing and potential customers. Furthermore, LinkedIn, as a platform used intensely by Business Developers from the industry, will be used to share news about the industry, promote new features/updates, events where the company will be present.

To guarantee a good SERP (Search Engine Result Page), all the content (key-words) of the website pages will be in line with *SEO (Search Engine Optimisation)* – on-site² and off-site³-, and *SEM (Search Engine Marketing)* (keywords) strategies, to guarantee that FraudProof website is duly optimised and gets strong organic search results, by being one of the first pages to appear in search engines, such as Google.

Moreover, in FraudProof's long term strategy, the company will invest in retargeting, a retention and conversion technique of online advertising. Through the use of a cookie-based technology that saves visitors' information, retargeting shows ads to specific users that were previously identified and are already acquainted with the brand. For instance: FraudProof website visitors, competitors' website visitors or FraudProof platform churn users.

It is considered a long term strategy because retargeting is more effective when the website and platform have a consistent number of daily visitors, which would create a more effective retargeting campaign. Retargeting is considered to be worthy as it targets specific users on controlled budgets. Normally, retargeting is done on LTV/CAC ratio⁴ basis. At this point, it is not possible to estimate such metrics.

² On-site SEO is the optimization of the website content and HTML.

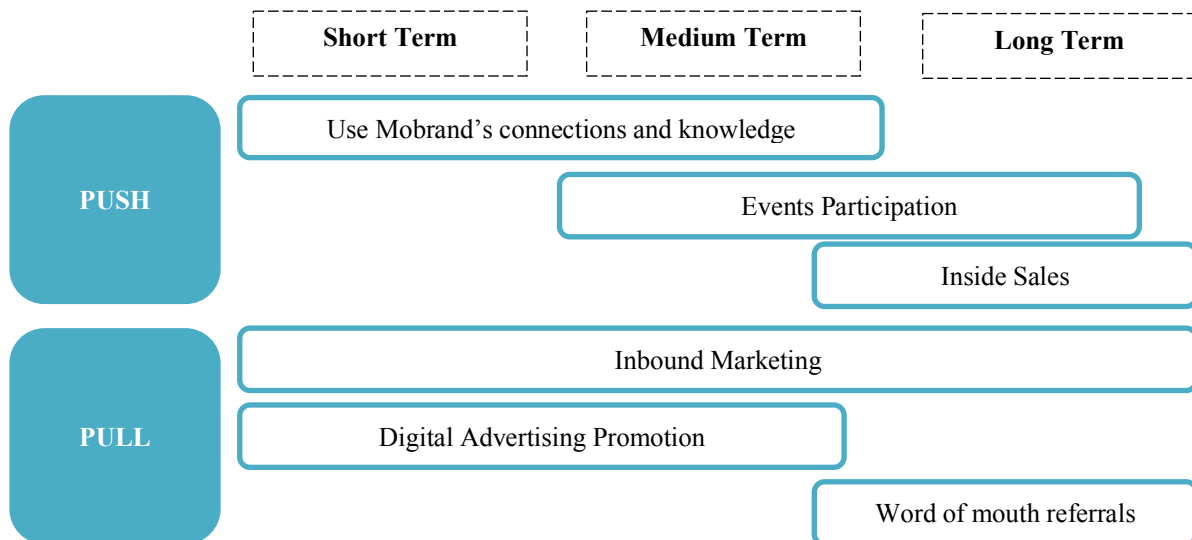
³ Off-site SEO is creating authority through building links, which means having other websites link to ours.

⁴ A healthy LTV:CAC ratio should 3:1, otherwise CAC is considered high.

15.1.4.1. Promotion Mix strategies

FraudProof will be promoted through a combination of promotion mix strategies – push and pull promotions. Figure 7 synthetizes the actions developed either in push and pull strategy in short, medium and long term.

Figure 7 – Push and Pull Strategy



Source: The Author, 2018

Push strategy

The Push strategy will focus on using Mobrand's existent connections, sales force, and insights of the mobile ad industry to push the product through the channels. A direct approach to reach customers, taking advantage of Mobrand's client knowledge.

To promote the company and develop new business, the company will be present, as an attendant or exhibitor, in several events of the industry, such as Dmexco (Germany), Affiliate Summit West (USA), Affiliate Summit East (USA), Apps World (United Kingdom), App Promotion Summit (Germany), Mobile Monetization Summit (Israel).

Pull Strategy

The company will also follow a pull strategy, using *Inbound Marketing*⁵ activities to attract consumers to buy the product, instead of reaching out to them. Inbound marketing

⁵ Inbound Marketing Strategy methodology was popularized by HubSpot, an American company founded in 2006, considered one of the world's leading inbound marketing and sales platform.

methodology is about creating a customer journey that adds value and creates trust and credibility for the business.

It is about attracting prospects and clients to the website, engaging with them, creating esteemed experiences and building trust in the brand from the very first moments. Inbound Marketing methodology can be divided into four main phases:

- a) **“Attract”** – Attract strangers to the business,
- b) **“Convert”** – Convert visitors into leads,
- c) **“Close”** – Close the sale, turning leads into customers,
- d) **“Delight”** – Delighting customers continuously so that they start promoting themselves the product to other people (referrals).

And three main stages:

- a) **“Awareness stage”** – in this stage, the prospect is starting to realize or identifying that there is a problem they need to solve and, as such, they will start to look for solutions.
- b) **“Consideration stage”** – in this stage, the prospect knows their problem and is actively researching the available market options to solve the problem.
- c) **“Decision stage”** - in this stage, the prospect will narrow down the list of different options available and ultimately decision which one will purchase.

In Annex LVI, one can find a representation of the four phases as well as the buyer’s journey stage – awareness, consideration, decision. (See Annex LVI – Inbound Marketing Methodology – The Author, 2018).

In order to attract the strangers and create awareness of the product, FraudProof Inbound Marketing will follow develop a set of actions. It is planned a continuous content creation strategy that will feed not only the platform social networks as well as the website blog. This will allow FraudProof to develop closer relationships with potential consumers, brand awareness and authority in the industry, through SEO. Moreover, the website and platform will have live chat service that will create a good customer experience while being able to collect valuable insights about the customer and its journey inside FraudProof. FraudProof will also make efforts to make a presence in B2B review websites, since prospects are used to searching online for other people’s opinion on products/services before purchasing. In this sense, actual customers will be encouraged to leave their comments in such channels.

To convert visitors into leads, FraudProof will leverage its 30 days free-trial package through the use of CTA in the website and promoting it in their social media pages. This strategy will result in a greater number of registrations and activity on the platform. Having the opportunity to know the service without strings attached will build a sense of security and proximity between user and FraudProof. Likewise, CTA buttons and forms alongside the website will be used to support user conversion. These actions will allow to collect more data on the prospect, fostering a more personalized approach.

FraudProof will also resort to the use of email marketing to maintain regular contact with leads that are using the free trial and, as such, are hypothetically about to become customers. Email marketing will take the form, for example, of tips on how to use the platform and how to get the most out of its tools. In a non-aggressive way, FraudProof will also suggested to schedule a meeting with the prospect to evaluate their experience, main needs, taking advantage of the opportunity to close the deal.

To delight its customers, the Platform will distribute personalized satisfaction surveys to its customers with the purpose of evaluating the customers overall satisfaction and, namely, the suggestions they might have to expand its experience. Additionally, FraudProof will continue to develop a strong presence on its social media pages, updating constantly its blog contents, sharing its knowledge with the industry.

Table 14 resumes the type of actions to be developed throughout the main stages and phases of Inbound Marketing.

Table 14 – Inbound Marketing Strategy

Stage	Phase	Action	Channel	Goal
Awareness	Attract	Presence in B2B review websites	Review Websites	Prospects usually search reviews about products/services in an initial phase, thus it is important to encourage customers to review the service
		Live chat service with team and bot support, that is also gathers user useful information	Website	Connect, converse and create a relationship with prospects, demonstrating great customer experience.
		Social Media Regular Postage - news about the industry, promote new features/updates, events where the company will be feature.	LinkedIn, Twitter, Facebook	These platforms will be useful to create brand awareness and promote the brand itself, reaching existing and potential customers.
		Content Creation – blog posts, infographic content, learning library, how-to guides, case studies, client reference, videos.	Website Blog, shared also in social media pages	Build authority in industry and SEO ranking (keywords), while creating brand awareness.
Consideration	Convert	FraudProof free-trial package during 30 days	Website ->Platform	Engage with prospects, by giving them the opportunity to use the platform for free and eventually acquiring new customers.
		Use of conversion tools – CTAs, forms	Website, Platform	Capture and save prospect information, personalizing the buyer's journey experience
	Close	Email marketing: Tips on using the platform, explaining the platforms main features and how to take advantage of them, while prospects are using the free-trial.	Email	Keep in touch with the prospects that are currently using the 30-days free trial, helping them to take full advantage of the platform, in order to close the sale.
		Sending customers a reminder when their trial period is coming to an end.		
Decision	Delight	Meeting scheduling with prospecting	CRM and videoconference	Getting to know customers' needs and wants, while showcasing main advantages of the product.
		Distribution of personalized satisfaction surveys	Email or Platform	Assess and evaluate customer satisfaction, expectations and suggestions in relation to the platform

Source: The Author, 2018

15.1.5. People

Currently, Mobrand is composed by a small team of 10 people (See Annex LVII – Current organization of Mobrand – The Author, 2018). Its low-level hierarchal structure matches the dimension of the company, that aims to eliminate internal communication barriers and have a strong response to market changes.

Taking into account that the existing tech team does not have enough resources to take in a project of this dimension with the current structure, Mobrand would need to contract at least 4 professionals –Front-end Developer, Back-End Developer, Data Scientist and Designer -, to assist the development of FraudProof, alongside other members of the corporation. From Mobrand team and current payroll, at least three professionals need to be directly involved: CTO, COO and developer.

The CTO would initially assume the position of IT Product Manager. The IT Product Manager mission is to successfully coordinate the set-up of FraudProof SaaS product from the very beginning - create, manage, monitor and report on the project in order to meet the delivery date and the projected project quality. This job requires strong project leadership and communication skills, team work mentality and problem solving mindset. The COO would initially assume the position of Business Development Manager, being responsible for seeking and developing new sales opportunities, promoting the project. Amongst the job key responsibilities are: generate new leads, keep close communication with new and existing prospects, develop long-term business strategy, create monthly forecasts on revenue, report on revenue and on-going business opportunities. The BDM role will imply travelling to participate in important industry events such as DMEXCO (Germany), Affiliate Summit West (USA), Mobile World Congress (Barcelona), Ad Tech (India), Global Mobile Internet Conference (China), Affiliate World Asia (Thailand). Also, Mobrand's Back-End Developer would assist the newly contracted Back-End developer. Together, they will create a dynamic duo. Thus, to join Mobrand's current team, the following professionals will be necessary:

Back-End Developer

Reporting directly to the CTO/IT Project Manager and working alongside other members of the tech team, the back-end developer will be responsible for the development from scratch of

the FraudProof SaaS platform, being in charge for design, features implementation, bug fixes, code actualizations and the platforms overall operational health.

The Web Developer will collaborate within a small team and engage in discussions related with the SaaS product to ensure the vision of the Product Manager is met. The professional also needs to have excellent computer science knowledge in what concerns data structures, algorithms and system functional complexity (integration with other software, multiple user collaboration, visualization options, data states, management operations). This position should be filled by a professional who has a minimum 1 year experience in similar functions, with preferred BA degree in Software Engineering/Computer Science or related field.

This function is targeted for a exempt employee and presumes a 40 hours a week full time schedule, from Monday to Friday. The remuneration will be €1300 monthly, with a daily lunch allowance of €7,63.

Data Scientist

The data scientist will be responsible for ad hoc investigations, algorithm development, creating and iterate platforms dashboards. This professional is also responsible for extract insights and knowledge from the data collected by the company on a daily basis, to help the business scale its operation.

This position, that requires data analysis kills and data programming ability, will be filled by a professional with a preferred BA in data science or similar field and proven experience in machine learning, programming, data analysis.

The data scientist position presupposes a weekly schedule of 40 hours, full-time, from Monday to Friday, with a monthly remuneration of €1400 and a daily lunch allowance of €7,63.

User Experience (UX) and User Interface (UI) Designer

The UX Designer will ensure that the FraudProof SaaS product is user friendly, has a cohesive and logical experience flow and provides a great user experience. The designer will be responsible for user interface (UI) design, ensuring that the visual elements are aligned with the desired UX experience.

The designer will work with the Software Developer and the IT Project Manager, reporting directly to the CTO. The candidate must be a team player, detailed oriented, strong communication skills when it comes to UX/UI concepts and reasoning and have working knowledge of the standard UX design tolls. Requirements wise, a BA degree in related field is

mandatory, as well as a minimum 1 year of dedicated field experience in creating user experience wireframes.

UX/UI Designer position is directed for an exempt employee with a working schedule of 40 hours a week, from Monday to Friday. The remuneration will be €1100 monthly, with a daily lunch allowance of €7,63.

Front-End Developer

The front-end will be responsible for implementation of all the visual elements with which the clients will see and interact. This professional will need to develop high quality software for FraudProof Platform, develop REST API's, elaborate technical documentation.

It will work closely with the back-end developers, given these proximity of these roles, with the Product Manager and also with the designer in order to guarantee the UI and UX goals. Regarding technical skills, the professional needs to have experience with front-end technologies (HTML5, CSS3, SASS) and JavaScript (React, Polymer, Angular, jQuery, others). This position should be filled by a professional who has a minimum 1 year experience in similar functions, with preferred BA degree in Computer Science or related field.

This position presupposes a weekly schedule of 40 hours, full-time, from Monday to Friday, with a monthly remuneration of €1300 and a daily lunch allowance of €7,63.

Table 15 – Expenses with People

Expenses with People and Payments	€				
	Monthly Remuneration (Gross)	Year 1	Year 2	Year 3	Year 4
Back-end Developer	1.300	18.200	18.200	18.200	18.200
Front-End Developer	1.300	18.200	18.200	18.200	18.200
UX/UI Designer	1.100	15.400	15.400	15.400	15.400
Data Scientist	1.400	19.600	19.600	19.600	19.600
TOTAL		71.400	71.400	71.400	71.400
Other expenses					
Lunch Allowance	160,23	7.050,12	7.050,12	7.050,12	7.050,12
Social Security Contribution	23,75%	19.783,8	19.783,8	19.783,8	19.783,8
Worker Accident Insurance	1,5%	833	833	833	833
TOTAL PEOPLE EXPENSE		99066.9	99066.9	99066.9	99066.9

Source: The Author, 2018

15.2. Technical Aspects

15.2.1. Technology

FraudProof project will imply a very strong technological component, given its value proposition. As the platform will be the visible face of the service, there are some strategies that need to be followed in what concerns technology:

1. Ensure that the SaaS infrastructure hosting option chosen for the FraudProof platform delivers both on performance, scalability and availability. This is very important because the platform will demand it on several aspects either by its customers – for example, when they make requests through the platform (*front-end*), requiring enormous amounts of data to be processed in a short amount of time-, by its employees – when they are using backoffice-, or even by its own internal mechanisms and procedures.
2. Make sure that FraudProof platform is a well-oiled agile machine that provides a good navigation experience, information structure and visual identity.
3. Guarantee that the technology, developed or outsourced, facilitates the streamlining process in Sales and Marketing.

To guarantee the first point, FraudProof will contract dedicated servers instead of other options available like cloud platforms or even owned hardware. Compared to the other solutions, dedicated servers are considered to have more performance (more powerful CPU, lower latency and more storage) at a moderate fair price-points that also permit scalability. On the down side, this decision implies server management and monitorization, which removes some time from the project development itself.

FraudProof will take advantage of two dedicated servers that Mobrand can spare, however, it will need to contract, at least, more 3 servers. For that effect, FraudProof will contract the services of a company named OVH, which owns 27 datacenters worldwide. With each server costing €120 per month, total servers expenses will be €360 per month. FraudProof's platform will require access to more servers' than the website mainly due to the necessity of data storage, computation, backoffice, heavy analysis burden, amongst other. In order to guarantee the second point, the IT Product Manager will have a key role to ensure that the all tech team (*back-end and front-end developers*) is on the same when it comes to ensure the project goals.

To deliver the third point, all the technology to be developed must be built in such a way as to be used in the company sales favor. FraudProof should be able to make sense of the data and insights collected to deliver even more value to its customers or prospects. In that sense, and to better acquire and retain customers, the company will contact a live chat service that will emphasize the company customer experience. Crisp is the company that will provide that service – Crisp –, and charges €95 per month.

Even though the project will take advantage of technological structure already existent at Mobrand, such as servers and high-speed internet in Lisbon offices, there are other associated business needs, as a IP address database, which lays the foundation for detecting IP addresses that are associated with fraudulent activity, such as bots, datacenters. Dbip would be the company selected to provide such service for €99.99 per month.

Overall, the initial infrastructure necessary to launch FraudProof would be €555 per month, €6660 per year (see Table 16).

Table 16 - Technological Expenses

Expenses With Technologic Infrastructure				€
	Year 1	Year 2	Year 3	Year 4
3 Servers	4.320	4.320	4.320	4.320
IP database	1.200	1.200	1.200	1.200
Live Chat Service	1.140	1.140	1.140	1.140
TOTAL TECHNOLOGY EXPENSE	6.660	6.660	6.660	6.660
TOTAL PEOPLE + TECH EXPENSE	105.727	105.727	105.727	105.727

Source: The Author, 2018

16. Fundamentals for Implementation

In order to estimate the commercial launch of FraudProof and also map the most important steps of this project, an implementation chronogram was planned (see table 17). The implementation phase of FraudProof will occur between the end of 2018 and during the year 2020, when it is expected to officially launch the anti-fraud SaaS platform.

Table 17 - Project Implementation chronogram

	2018				2019												2020											
	SEPT	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEPT	OCT	NOV	DEC
Business Plan Elaboration																												
Brand Trademark																												
Recruitment																												
Architectural Planning of FraudProof Platform																												
SaaS Platform and Website Development																												
Bug fixes																												
Beta Launch of FraudProof Platform																												
Commercial Launch of FraudProof Platform																												

Source: The Author, 2018

The first 6 months will be devoted to the creation of this project, the registration of the trademark, the recruitment of the necessary elements and the architectural planning of the platform. The following 10 months will be dedicated entirely to the most operational phase of the project, which is linked to the development of the FraudProof technology, platform and website.

Analyzing the implementation timeline, it is evident that the first phase of the project is linked to the creation of the present business plan, which it is expected to be completed during the month of December. In that same month, the FraudProof brand will be registered.

The recruitment process is planned to start during the months of November and January. After that, the newly joined members alongside Mobrand's designated members can start to discuss and brainstorm together about the architecture of FraudProof technology, platform and website. This phase is considered very important, as it is the foundation of the project, and will take a whole month.

Once this is done, the most operational period of the project takes place. FraudProof team will take 7 months to design from scratch the service anti-fraud technology, website and platform. This phase is crucial for the success of the project.

Afterwards, three months will be dedicated to debug phase, which consists of search and correcting bugs and errors. At the same time, it is expected to Beta launch FraudProof platform. During this period, beta users will test the service and ensure that there is no barrier to the commercial launch of the project.

Completed the most time consuming and demanding phase of the project, FraudProof will be able to be officially launched in January 2020.

17. Operational Analysis

17.1. Expenses

Table 18 - Expenses Map

Expenses with People and Payments					€
	Monthly Wage	Year 1	Year 2	Year 3	Year 4
Back-end Developer	1.300	18.200	18.200	18.200	18.200
Front-End Developer	1.300	18.200	18.200	18.200	18.200
UX/UI Designer	1.100	15.400	15.400	15.400	15.400
Data Scientist	1.400	19.600	19.600	19.600	19.600
TOTAL		71.400	71.400	71.400	71.400
Other expenses					
Lunch Allowance	160.23	7.050.1	7.050.12	7.050.12	7.050.1
Social Security Contribution	23,75%	19.784	19.783.8	19.783.8	19.784
Worker Accident Insurance	1,5%	833	833	833	833
TOTAL PEOPLE EXPENSE		99.066.9	99.066.9	99.066.9	99.066.9
Expenses With Technologic Infrastructure					
	Year 1	Year 2	Year 3	Year 4	
3 Servers	4.320	4.320	4.320	4.320	
IP database	1.200	1.200	1.200	1.200	
Live Chat Service	1.140	1.140	1.140	1.140	
TOTAL TECH EXPENSE	6.660	6.660	6.660	6.660	
TOTAL PEOPLE + TECH EXPENSE	105.727	105.727	105.727	105.727	

Source: The Author, 2018

17.2. Investment

This project assumes a total necessary investment of 6.265€ for FraudProof to operate (See Table 19). The company will need to invest in equipment, namely in four computers for the new company members, which will cost €6.000.

Also, the company will spend 250€ in Industry Propriety to register FraudProof trademark in Portuguese territory. Lastly, the register of the domain of the website, with an annual cost of 15€.

Table 19 - Investment Map

Investment	€			
	Year 1	Year 2	Year 3	Year 4
Equipment				
Computers	6.000	/	/	/
Industrial Propriety				
Trademark Register	250	-	-	-
Other Investments				
Domain Register	15	15	15	15
TOTAL	6.265	15	15	15

Reinvestment costs are not considered during the company's activity. Given that the analysis of this project is of only four years, the company believes that the equipment assets – computers specifically –, will continue to work perfectly, even though the useful life cycle of these assets are estimated, accounting wise, to depreciate over the period of three years.

17.3. Sales Forecast

To determine the project sales of FraudProof, it is crucial to collect market information. Given the lack of information available to assess the number of mobile ad companies operating worldwide, the author considered that the number of partners working with the main mobile ad trackers companies to be a good metric because of their compulsory role in this industry. As such, the total market will be defined through this scope (See Table 20).

Table 20 – Market dimension according to mobile trackers

Mobile Tracker	Number of Integrated Partners
Appsflyer	> 4000 partners
Kochava	>3800 partners
Adjust	> 900 partners

Source: Appsflyer, Kochava and Adjust (2018)

To reach the number of clients that FraudProof would have in its first year of activity, the author assuming that:

- Around 50% of total estimated market would be interested in FraudProof services.
- 30% of those companies are reachable and would be capable to purchasing any package.

- 15% of the available market is what FraudProof expects to reach in the first year of activity.

Table 21 – Potential Market-target size of FraudProof

Number of companies	8700 potential customers		
Total market	100%	8700	All potential buyers of FraudProof
Potential Market	50%	4350	Number of companies with interest in the product
Available market	30%	1305	Companies who are reachable
Market for the first year	15%	196	Number of companies FraudProof expects to reach in the first year

Source: The Author, 2018

After assuming a percentage of annual growth for the following years, the number of clients for the next four years were obtained. The growth rates are expected to be higher in the first years due to marketing investments and, afterwards, the growth rates are expected to decrease mainly due to overall service development stabilization (See Table 22).

Table 22 – Growth Rates

		Year 1	Year 2	Year 3	Year 4
Growth	% of maximum growth		30%	25%	15%
Clients	Number of clients	196	255	319	366

Source: The Author, 2018

In order to reach the final values for the sales, one needs to take into account that the service has packages to serve a wide range of market-target. The table below does not contemplate the additional conversions costs neither the custom package expected sales, given that is difficult to forecast such extras. The extra conversions and the custom package would have a positive impact in the sales value, that is not taking into account in this analysis.

The author assumed that the price of the packages would impact directly the number of sales. Thus, the higher numbers of sales are more concentrated in the lower pricing packages, which gives an inverted pyramid look to it (See Table 23).

Table 23 - Sales prediction map (in US \$)

Services	Year 1	Year 2	Year 3	Year 4
N° of Basic Package	91	118	148	170
Sales (\$350/each)	31.850	41.300	51.800	59.500
Pro Package	65	85	106	121
Sales (\$750/each)	48.750	63.375	79.219	91.102
Entreprise Package	36	47	59	67
Sales (\$1550/each)	55.800	72.540	90.675	104.276
Expert Package	4	5	7	8
Sales (\$2500)	10.000	13.000	16.250	20.000
TOTAL Sales US \$	146.400	190.215	237.944	274.878
TOTAL number of Clients	196	255	319	366

Source: The Author, 2018

17.4. Evaluation

This project is based on a four-year projection, which reflects the period from January 2020 to December 2023. Given that the development of the FraudProof will not change Mobrand's financial structure, a sales projection was made to analyze the potential turnover that the project would contribute to the company's overall financial results.

Considering the project has estimated sales of 126.596€ in the first year and that its total costs are anticipated in 105.727€, the company believes to reach in its first year a revenue of 20.868€, therefore being able to recover the initial investment of 6.265€, and still generate a profit of 14.604€. As we can see from the table 24⁶, these results show that the project is economically viable and brings value to Mobrand.

Table 24 – Four year projection

	Year 1 €	Year 2 €	Year 3 €	Year 4 €
Sales	126.596	164.575	205.719	237.611
Expenses	105.727	105.727	105.727	105.727
Revenue	20.869	58.848	99.992	131.884
Investment	6.265	15	15	15
Profit	14.604	58.833	99.977	131.869

Source: The Author, 2018

⁶ Currency conversion made on 13/10/2018 where 1 USD = 0.864359 EUR

18. Project Conclusions

Across the globe, marketing budgets have been increasingly shifting to mobile as this dominant channel consumption habits continues to grow. Whilst this trend emerged, so did fraudsters. The realignment of budgets and the focus on mobile apps fuelled the rising of fraud, that is now a multi-billion dollar problem in the mobile ad ecosystem.

Despite the increased efforts to fight this trend, marketers acknowledge that fraudsters continue to snatch large portions of their ad budgets and observe with concern the rampant advances fraud made in the mobile ecosystem. To face this threat, marketers must be familiarized with the most common fraud tactics and protect themselves by allocating more resources to fraud prevention.

The growth of the mobile fraud industry has created a clear business opportunity for preventive and detection solutions to appear in the landscape. This project is a marketing plan of the launching of FraudProof, a SaaS anti-fraud platform designed to help CPI mobile companies to fight mobile ad fraud.

It is important to highlight that this new business unit being developed inside Mobrand ends up taking advantage of its structure, knowledge, insights and connections, which allow a vigorous competitive advantage, compared to potential new competitors.

Actually, there are established anti-fraud solutions operating in the industry, with solid brand image and international recognition. In view of the fact that FraudProof is a B2B service, there is a competitive atmosphere that will tend to intensify over the years, with attempts of players to strangle competitors' margins by decreasing prices.

The biggest setback that FraudProof will have to deal with is directly linked to Mobrand's activity as an Ad network. However, since the company already launched another independent tool – OfferTest –, the author considers that this obstacle will lose importance in the future.

The rapid technological and market change adds both a positive and negative note to the project. On one hand, it will demand constant alterations loops to the project that relies on a

heavy technological architecture. Additionally, there is the danger of missing out on new and important market trends. On the other hand, it is the motor of the industry and society, that needs and wants more innovative solutions.

The survey conducted and distributed to marketers online allowed to understand that they accept mobile ad fraud as a business cost of capitalizing this channel. Even though they are taking measures to tackle suspicious activity and expect more resources to be allocated in the following year to accelerate fraud mitigation, the great majority marketers believe that mobile fraud is very likely to increase in 2019. Yet, one third of respondents admitted to not contract any external anti-fraud tools.

Marketers answers also played a fundamental role in defining the core characteristics of FraudProof technology. To be true to respondents' expectations, the anti-fraud solution will need to have good quality, be innovative and easy to use product. Equally, FraudProof will pursue an aggressive market approach, with a penetration pricing strategy, in order to attract established and new customers. It will leverage of existing Mobrand's connections to facilitate the launch of the new business unit. To provide both quality and a low cost price, a thorough cost and quality control needs to be followed to not compromise these aspects.

The insights of the survey were deeply taken into account when designing the architecture of the product. Besides providing a full funnel mobile fraud detection, FraudProof will further stand out due to its real-time capabilities, predictive machine learning algorithms, and seamless integration.

FraudProof promotion, through the use of push and pull strategies, will have an influence in creating a valuable customer journey. The author believes that the use of inbound marketing will provide a strategic advantage, namely through the website blog constant alongside a frequent social media postage, the live chat service and the free-trial packages.

Likewise, the technological component of the project needs to meet the platform and user requirements. As such, its SaaS infrastructure needs to ensure performance, scalability and availability in order to guarantee a good user experience and smooth the marketing and sales process.

The author is aware of the operational analysis limitations, namely the delimitation of the size of the market based on the number mobile attribution companies. This is due to the lack of information of an industry that is considered global and, therefore, fragmented. Given the level of uncertainty, the sales projections assumptions and growth rates of the project take that into account.

Through the operational study performed, the author concludes that FraudProof is economically viable, being able to recover the initial within the first year of the project activity and to generate a profit of 14.604€, with an initial market reach of 196 companies.

19. Project Limitations

There are some important limitations that should be taken into account when reading this work.

Firstly, there is little information available about mobile advertising and mobile ad fraud. Given that it is quite a recent, complex and ever-changing industry, it is difficult to find information to support the literary review.

Secondly, the fact that this industry is dominated by privately held companies made the overall research harder. For instance, in the competition analysis, the author was not able to access all the desired information, as some corporations do not disclose some information related with their technology, pricing points and requested further contact, like calls, to deliver such information.

Thirdly, and lastly, due to the global scale of action and fragmented industry, it is very hard to assess the numbers of CPI mobile advertising players. For the purpose of estimating sales, the author appealed to mobile app attribution companies. These companies have an essential role in the entire ecosystem as an unbiased attribution authority, which means they are responsible for accrediting the appropriate media partner for actions such as app installs. So, to estimate the market dimension, the number of partners of the three most used trackers were considered. However, their values are based on information shared by the companies, that not always disclosed which partners are those exactly. Therefore, the market scope is not completely accurate as there is the risk of repeated or even off target companies. Still, that said, it is important to mention that the author believes the potential market-target to be larger. As such, the sales forecast assumptions are cautious and fairly conservative due to the mentioned limitations.

20. References

Books

Bouزيد, A. & Rennyson, D. 2015. *The art of SaaS: A Primer on the Fundamentals of Building and Running a Successful SaaS Business*.

Bush, O. 2015. *Programmatic advertising: The successful transformation to automated, data-driven marketing in real-time*. Springer

Chiong, K. X., & Chen, R. Y. 2016. *An empirical model of mobile advertising platforms*.

Daswani, N., Mysen, C., Rao, V., Weis, S., Gharachorloo, K. & Ghosemajumder, S. 2008. *Online advertising fraud. Crimeware Underst. New Attacks Defenses*. 40: 1–28

Hakansson, H. & Snehota, I. 1995. *Developing Relationships in Business Networks*.

Jakobsson, M. & Ramzan, Z., 2008. *Crimeware: understanding new attacks and defenses*. Addison-Wesley Professional.

Kotler, P., Armstrong, G., Harris, L. & Piercy, N. 2005. *Principles of marketing*. (4th European edition). Harlow: Financial Times.

Kshetri, N. 2010. *The economics of click fraud*. IEEE Security & Privacy, 8: 45-53.

Kumar, S. 2016. *Optimization Issues in Web and Mobile Advertising*, Texas: Springer

Lindon, D., Lendrevie, J., Lévy, J, Dionísio, P. and Rodrigues, J.V. 2004. *Mercator XXI – Teoria e Prática do Marketing*. Lisboa: Dom Quixote

Lynch, R. L. 2009. *Strategic management* (5th edition). UK: Pearson Education Limited.

Napier, H. A., Rivers, O. N., & Wagner, S. 2005. *Creating a winning e-business*. Cengage Learning.

Nazerzadeh, H., Saberi, A., & Vohra, R. 2013. ***Dynamic pay-per-action mechanisms and applications to online advertising***. Operations Research, 61: 98-111.

Porter, M. 1985. ***Competitive Advantage***, 1: 11-15. New York: The Free Press. Routledge, London.

Turban, E., King, D., Lee, J. K., Liang, T. P., & Turban, D. C. 2015. ***Electronic commerce: A managerial and social networks perspective***. Springer.

Yacob, F. 2015. ***Paid Attention: Innovative Advertising for a Digital World***. Kogan Page

Yuan, S., Abidin, A. Z., Sloan, M., & Wang, J. 2012. ***Internet advertising: An interplay among advertisers, online publishers, ad exchanges and web users***.

Zhu, X., Tao, H., Wu, Z., Cao, J., Kalish, K. & Kayne, J., 2017. ***Fraud Prevention in Online Digital Advertising***. Heidelberg: Springer.

Periodicals

Anderson, J.C. & Narus, J.A. 1998. Business marketing: understand what customers value. ***Harvard Business Review***, 76: 53–67.

Barnes, S. J., & Scornavacca, E. 004. Mobile marketing: the role of permission and acceptance. ***International Journal of Mobile Communications***, 2: 128 –139.

Bughin, J., 2014. Brand success in an era of digital Darwinism. ***Journal of Brand Strategy***, 2: 355-365.

Cho, G., Cho, J., Song, Y., Choi, D., & Kim, H. 2016. Combating online fraud attacks in mobile-based advertising. ***EURASIP Journal on Information Security***, 2016: 2.

Chong, F. & Carraro, G., 2006. Architecture strategies for catching the long tail. ***MSDN Library***, Microsoft Corporation: 9-10.

Clair, G.S., 2008. Software-as-a-Service (SaaS): Put the Focus on the KM/Knowledge Services Core Function. *AN EOS International white paper*.

Coviello, N.E. & Brodie, R.J. 2001. Contemporary Marketing Practices of Consumer and Business-to-Business Firms: How Different are they? *Journal of Business & Industrial Marketing*, 16: 382–400.

Cudmore, B. A., McCoy, J., Shuhy, J., & Taylor, J. 2009. Engaging online consumers with an interactive cost-per-action advertising model. *Journal of Internet Commerce*, 8: 288-308.

Edelman, B. 2014. Pitfalls and Fraud in Online Advertising Metrics: What Makes Advertisers Vulnerable to Cheaters, and How They Can Protect Themselves. *Journal of Advertising Research*, 54: 127–132.

Estrada-Jiménez, J., Parra-Arnau, J., Rodríguez-Hoyos, A., & Forné, J. 2017. Online advertising: Analysis of privacy threats and protection approaches. *Computer Communications*, 100: 32-51.

Evans, D. S. (2009). The online advertising industry: Economics, evolution, and privacy. *Journal of Economic Perspectives*, 23: 37-60.

Flosi, S., Fulgoni, G. & Vollman, A. 2013. If an advertisement runs online and no one sees it, is it still an ad? *Journal of Advertising Research*, 53:192-199.

Friedrich, R., Gröne, F., Hölbling, K. & Peterson, M. 2009. The march of mobile marketing: new chances for consumers companies, new opportunities for mobile operators. *Journal of Advertising Research March*: 54-61.

Fulgoni, G. 2015. The Rise of the Digital Omnivore. What It Means for Advertisers, Publishers, and App Developers. *Journal Advertising Research*, 55: 115-119.

Fulgoni, G. 2016. Fraud in Digital Advertising: A Multibillion-Dollar Black Hole: How Marketers Can Minimize Losses Caused by Bogus Web Traffic. *Journal of Advertising Research*, 56:122-125.

Guo, Z. & Ma, D., 2018. A model of competition between perpetual software and software as a service. *MIS Quarterly*, 42:1.

Haider, C. M. R., Iqbal, A., Rahman, A. H., & Rahman, M. S. 2018. An ensemble learning based approach for impression fraud detection in mobile advertising. *Journal of Network and Computer Applications*, 112: 126-141.

Haghirian, P., Madlberger, M. & Inoue, A., 2008. *Mobile Advertising In Different Stages Of Development: A Cross-Country Comparison Of Consumer Attitudes*. In Hawaii International Conference on System Sciences, Proceedings of the 41st Annual.

Hamad, H., Elbeltagi, I., Jones, P., & El-Gohary, H. 2015. Antecedents of B2B E-Commerce Adoption and its Effect on Competitive Advantage in Manufacturing SMEs. *Strategic Change*, 24: 405-428.

Hu, Y., Shin, J., & Tang, Z. 2015. Incentive problems in performance-based online advertising pricing: cost per click vs. cost per action. *Management Science*, 62: 2022-2038.

Immorlica, N., Jain, K., Mahdian, M., & Talwar, K. 2005. Click fraud resistant methods for learning click-through rates. *In International Workshop on Internet and Network Economics*, 34-45. Germany: Springer.

Iqbal, M. S., Zulkernine, M., Jaafar, F., & Gu, Y. (2018). Protecting Internet users from becoming victimized attackers of click-fraud. *Journal of Software: Evolution and Process*.

Kannan, P.K. & Li, H. 2017. Digital marketing: A framework, review and research agenda. *International Journal of Research in Marketing*, 32: 22-45.

Lamberton, C., & Stephen, A. 2016. A thematic exploration of digital, social media, and mobile marketing: Research evolution from 2000 to 2015 and an agenda for future inquiry. *Journal of Marketing*, 80: 146-176.

Leppaniemi, M., & Karjaluo, H. 2005. Factors influencing consumers' willingness to accept mobile advertising: a conceptual model. *International Journal of Mobile Communications*, 3: 197-213.

Leppäniemi, M., Karjaluo, H. & Salo, J., 2004. The Success Factors Of Mobile Advertising Value Chain. *E Business Review*, IV: 93-97.

Lilien, G.L. 1987. Business marketing: present and future', *Industrial Marketing and Purchasing*, Vol. 2: 3-21.

Mamais, S. S., & Theodorakopoulos, G. 2017. Behavioural Verification: Preventing Report Fraud in Decentralized Advert Distribution Systems. *Future Internet*, 9: 88.

Matin, S. 2007. Clicks Ahoy! Navigating online advertising in a sea of fraudulent clicks. *Berkeley Technology Law Journal*, 533-554.

Mort, G. & Drennan, J., 2002. Mobile Digital Technology: Emerging Issues For Marketing. *Journal Of Database Marketing*, 10: 9.

Nicholson, D. 2018. Cloud first—tackling the security challenges. *Computer Fraud & Security*, 1: 8-11.

Oberoi, R. & Dey, S., 2017. Survey of Security Issues in Cloud based E-Commerce. *International Journal*, 7:5.

Persaud, A., & Azhar, I. (2012). Innovative mobile marketing via smartphones: Are consumers ready? *Marketing Intelligence & Planning*, 30:418-443.

Ratliff, J. D., & Rubinfeld, D. L. 2010. Online advertising: Defining relevant markets. *Journal of Competition Law and Economics*, 6: 653-686.

Rzemieniak, M., 2015. Measuring the effectiveness of online advertising campaigns in the aspect of e-entrepreneurship. *Procedia Computer Science*, 65: 980-987.

Soubusta, S., 2008. On Click Fraud. *Information Wissenschaft und Praxis*, 59: 136.

Yu, Y., Wang, X., Zhong, R. Y., & Huang, G. Q. 2016. E-commerce logistics in supply chain management: Practice perspective. *Procedia CIRP*, 52: 179-185.

Unpublished works

Abu Rajab, M., Zarfoss, J., Monroe, F., & Terzis, A. 2006. *A multifaceted approach to understanding the botnet phenomenon*. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement-

Dong, F., Wang, H., Li, L., Guo, Y., Bissyandé, T.F., Liu, T., Xu, G. & Klein, J., 2018. *Frauddroid: Automated ad fraud detection for android apps*. In The 26th ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering.

Iqbal, M. S., Zulkernine, M., Jaafar, F., & Gu, Y. 2016. *Fraud: Fighting click-fraud from the user side*. In High Assurance Systems Engineering (HASE), 2016 IEEE 17th International Symposium.

Juels, A., Stamm, S., & Jakobsson, M. 2007. *Combating Click Fraud via Premium Clicks*. In USENIX Security Symposium.

Nazerzadeh, H., Saberi, A., & Vohra, R. 2008. *Dynamic cost-per-action mechanisms and applications to online advertising*. In Proceedings of the 17th international conference on World Wide Web.

Rastogi, V., Shao, R., Chen, Y., Pan, X., Zou, S. & Riley, R., 2016. *Are these Ads Safe: Detecting Hidden Attacks through the Mobile App-Web Interfaces*. In Conference: Network and Distributed System Security Symposium.

Stone-Gross, B., Stevens, R., Zarras, A., Kemmerer, R., Kruegel, C., & Vigna, G. 2011. *Understanding fraudulent activities in online ad exchanges*. In Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference.

Yuan, S., Wang, J., & Zhao, X. 2013. *Real-time bidding for online advertising: measurement and analysis*. In Proceedings of the Seventh International Workshop on Data Mining for Online Advertising (p. 3). ACM.

Electronic documents

ACEPI. 2018. *Compras online em Portugal ascenderam a 4,6 mil milhões de euros em 2017*. Available at: http://new.acepi.pt/download.php?f=2018_01_30_%20PR_ACEPI_RESULTADOS_E_TEND%C4%82NCIAS_ECOMMERCE.pdf.

Applift. 2015. *Fighting Mobile Fraud In The Programmatic Era*. Available at: <http://insights.applift.com/fraud/>

Appsflyer. 2016. *Getting started with mobile attribution and marketing analytics*. Available at: http://cdn2.hubspot.net/hubfs/597489/Updated_Beginners_Guide_-_April_2016/Getting_Started_with_Mobile_Attribution_and_Marketing_Analytics_-_April_2016.pdf

Bagchi, M., Murdocha, S., & Scanlan, J. 2015. *The state of global media spending*. Available at: <https://www.mckinsey.com/industries/media-and-entertainment/our-insights/the-state-of-global-media-spending>

Banco de Portugal 2018. *Projections for the Portuguese economy: 2018-2020*. Available at: https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/proj_jun2018_e.pdf

ComScore. 2016. *The Value of a Digital Ad*. Available at: <https://www.aaaa.org/wp-content/uploads/2016/05/comScore-Value-of-Digital-Ad.pdf>

DESI. 2018. *Digital Economy and Society Index (DESI) 2018 Country Report Portugal*. Available at: www.dgae.gov.pt/gestao-de-ficheiros...ano.../desi_2018-country_profile_en-pdf.aspx

ERC. 2017. ***Growing up between screens: use of electronic devices by children (3-8 years)***.

Available at: <https://www.internetsegura.pt/sites/default/files/crescendo-entre-ecras.pdf>

Ericsson. 2017. ***Ericsson Mobility Report: 70 percent of world's population using***

smartphones by 2020. Available at: <https://www.ericsson.com/en/press-releases/2015/6/ericsson-mobility-report-70-percent-of-worlds-population-using-smartphones-by-2020>

Fox-Brewster , T. 2017. ***Google Just Killed What Might Be The Biggest Android Ad Fraud Ever***. Forbes Online. Available at:

<https://www.forbes.com/sites/thomasbrewster/2017/05/26/googleshuts-down-massive-ad-fraud-on-play-store/#4c61b8967807>

Gartner. 2018. ***Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.3 Percent***

in 2019. Available at: <https://www.gartner.com/en/newsroom/press-releases/2018-09-12-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2019>

Goldberg, L. 2017. ***Digital Ad Spend Reaches an All-Time High of \$88 Billion in 2017,***

With Mobile Upswing Unabated, Accounting for 57% of Revenue. IAB Online. Available at: <https://www.iab.com/news/digital-ad-spend-reaches-all-time-high-88-billion-2017-mobile-upswing-unabated-accounting-57-revenue/>

Hewlett Packard Enterprise. 2016. ***The Business of Hacking***. Available at:

<http://static.politico.com/b9/55/4e3ce4cc41d88401e264dcacc35c/hpe-security-research-business-of-hacking-may-2016.pdf>

HubSpot. ***Inbound marketing***. Available at: <https://www.hubspot.com/inbound-marketing>

IAB. 1997. ***Internet Advertising Sees Breakthrough Year in 1997***. Available at:

<https://www.iab.com/news/internet-advertising-sees-breakthrough-year-1997/>

Lella, A., & Lipsman, A. 2017. ***The 2017 U.S. Mobile App Report***. Available at:

<https://www.comscore.com/Insights/Presentations-and-Whitepapers/2017/The-2017-US-Mobile-App-Report>

Morrison, M. & Peterson, T. 2015. ***Yes, There Is A War On Advertising. Now What?***

Available at: <https://adage.com/article/print-edition/a-war-advertising/300336/>

Phillips, E. 2015. ***Retailers scale up online sales distribution networks.*** The Wall Street

Journal Online. Available at: <http://www.wsj.com/articles/retailers-scale-up-online-sales-distribution-networks-1447792869>

Silva, S. 2014. ***Mais de 70% dos jovens portugueses com sinais de dependência da Internet.***

Público Online. Available at: <https://www.publico.pt/2014/11/03/sociedade/noticia/quase-tres-quartos-dos-jovens-portugueses-apresentam-sinais-de-dependencia-da-internet-1674907>

Silva, S. 2014. ***O desafio agora é móvel.*** Available at:

<https://www.publico.pt/2014/11/03/sociedade/noticia/o-desafio-agora-e-movel-1674939>

StartApp. ***Winning the Fight Against Mobile Fraud.*** Available at:

<https://www.startapp.com/resource/whitepaper-winning-fight-against-fraud/>

Vidakovic, R. ***The Many Faces Of Programmatic Ad Fraud.*** Available at:

<https://marketingland.com/many-faces-programmatic-ad-fraud-142335>

Visão. 2018. ***80% dos jovens portugueses dizem "sentir-se mal" quando não estão online.***

Available at: <http://visao.sapo.pt/actualidade/sociedade/2018-05-07-80-dos-jovens-portugueses-dizem-sentir-se-mal-quando-nao-estao-online>

Word Federation of Advertisers. 2017. ***Compendium of ad fraud knowledge for media investor.*** Available at:

https://www.wfanet.org/app/uploads/2017/04/WFA_Compendium_Of_Ad_Fraud_Knowledge.pdf

World Travel & Tourism Council. 2018. ***Travel & tourism economic impact 2018 Portugal.***

Available at: <https://www.wttc.org/-/media/files/reports/economic-impact-research/countries-2018/portugal2018.pdf>

Websites

www.mobrand.com/

www.offertest.net/

www.pordata.pt/

www.statista.com

www.ine.pt/

www.acepi.pt/

www.anacom.pt/

www.erc.pt/

www.marktest.com/wap/

www.oecd.org/portugal/

www.wttc.org/

www.appsflyer.com/

www.adjust.com/

www.kochava.com

www.iab.com/

www.ec.europa.eu/eurostat

www.fraudscore.mobi

www.whiteops.com/

integralads.com/

www.24metrics.com/

www.fraudlogix.com/

www.impact.com/

www.ovh.pt/

www.crisp.chat

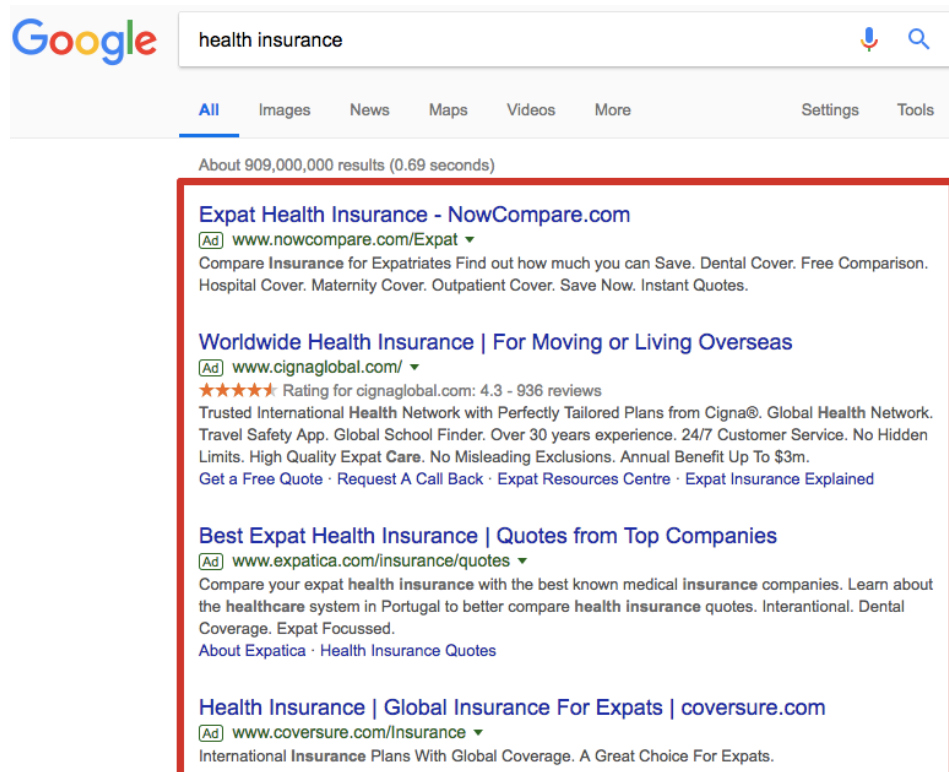
www.db-ip.com/

www.tune.com/

www.olamobile.com/

21. Annexes

Annex I – Search advertising example



Source: Google, 2018

Annex II – Display advertising example



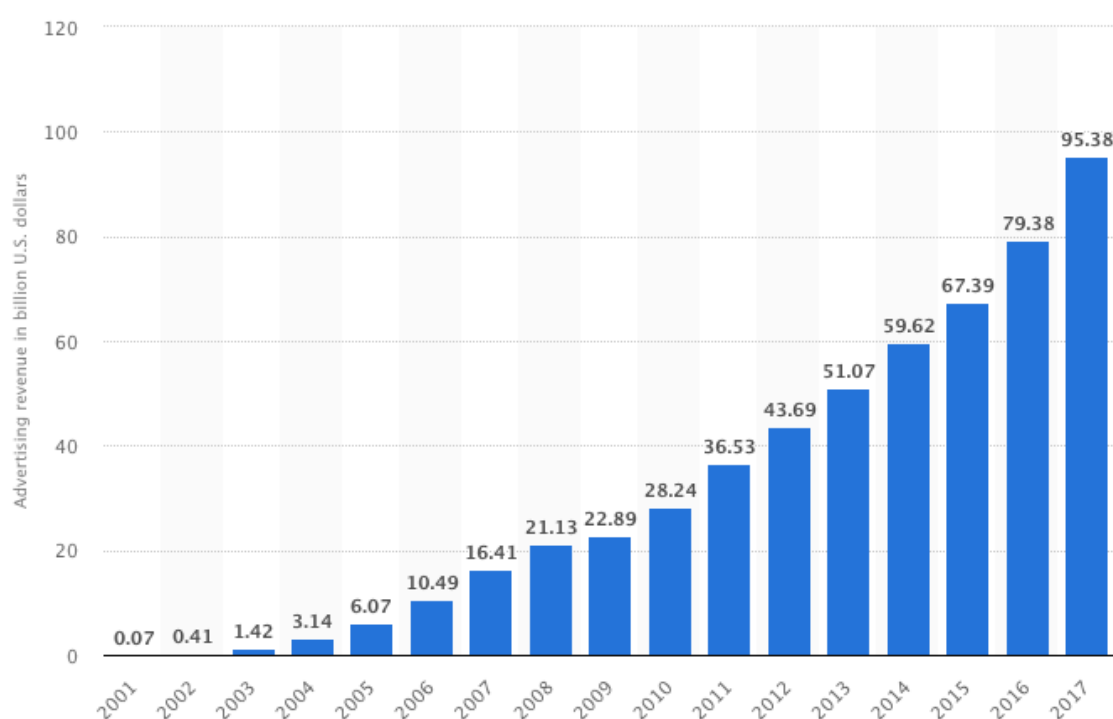
Source: Público, 2018

Annex III – Total global spending by category (US \$ millions), at average 2014 exchange rates

Category	2009	2010	2011	2012	2013	2014p	2009–2014p CAGR	2015	2016	2017	2018	2019	2014–2019 CAGR
Digital Advertising	60,336	70,756	81,544	94,065	109,686	127,345	16.1	146,617	168,538	190,822	211,955	231,442	12.7
Broadband	234,137	267,784	313,039	355,947	393,274	429,280	12.9	463,826	500,510	539,361	581,203	624,613	7.8
TV Advertising	136,792	152,824	159,985	168,749	173,314	183,501	6.1	189,445	202,511	208,960	223,099	233,876	5.0
In-Home Video Entertainment	257,841	270,985	283,287	297,662	310,783	323,408	4.6	331,922	347,781	358,950	370,244	381,648	3.4
Audio Entertainment	92,551	91,294	92,470	93,681	96,559	95,636	0.7	96,984	98,772	100,667	102,767	104,648	1.8
Cinema	30,147	31,692	32,245	34,719	35,972	37,133	4.3	39,359	41,614	43,799	45,834	48,334	5.4
Out-of-Home	24,817	27,044	27,816	29,150	30,627	31,747	5.0	33,220	34,824	36,468	38,337	40,334	4.9
Consumer Magazine Publishing	65,573	65,010	65,376	63,635	61,167	59,061	-2.1	57,640	56,546	55,710	55,080	54,610	-1.6
Newspaper Publishing	153,392	154,521	153,900	150,311	145,688	142,430	-1.5	140,647	139,917	140,023	140,766	141,968	-0.1
Consumer Books	69,687	70,034	69,504	69,944	70,750	72,357	0.8	72,976	74,020	74,794	75,425	75,968	1.0
Educational Publishing	38,619	39,608	40,135	39,347	39,955	40,980	1.2	41,624	42,138	42,629	43,241	43,929	1.4
Video Games	55,190	57,791	60,822	66,444	73,973	84,534	8.9	94,117	103,454	111,634	118,738	124,542	8.1
Total	1,208,470	1,286,526	1,364,933	1,446,077	1,521,420	1,603,951	5.8	1,681,314	1,779,536	1,868,556	1,966,897	2,061,479	5.1

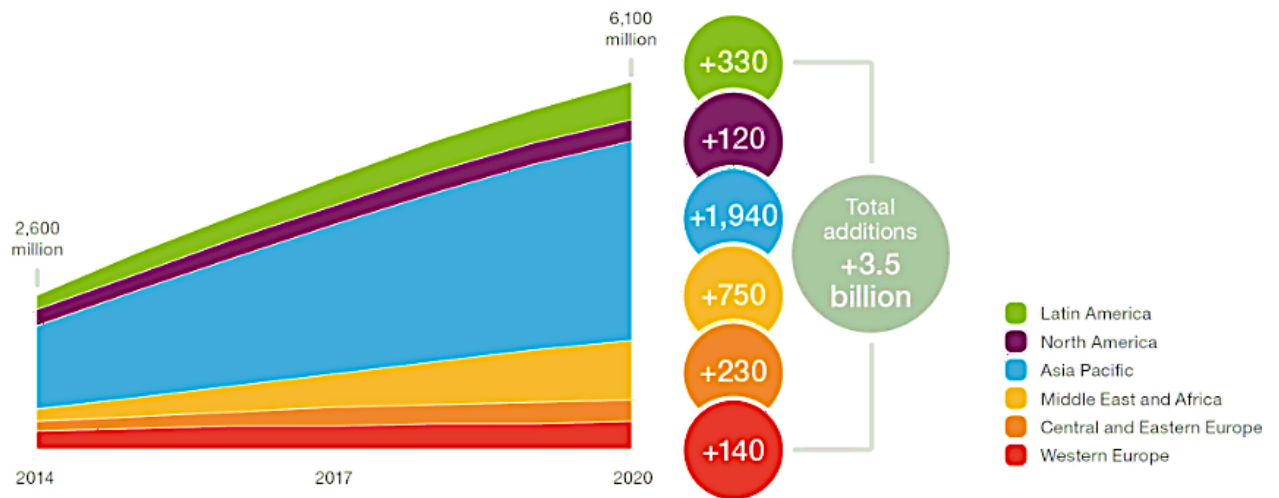
Source: McKinsey & Company, 2015

Annex IV – Google's ad revenue between 2001 and 2017



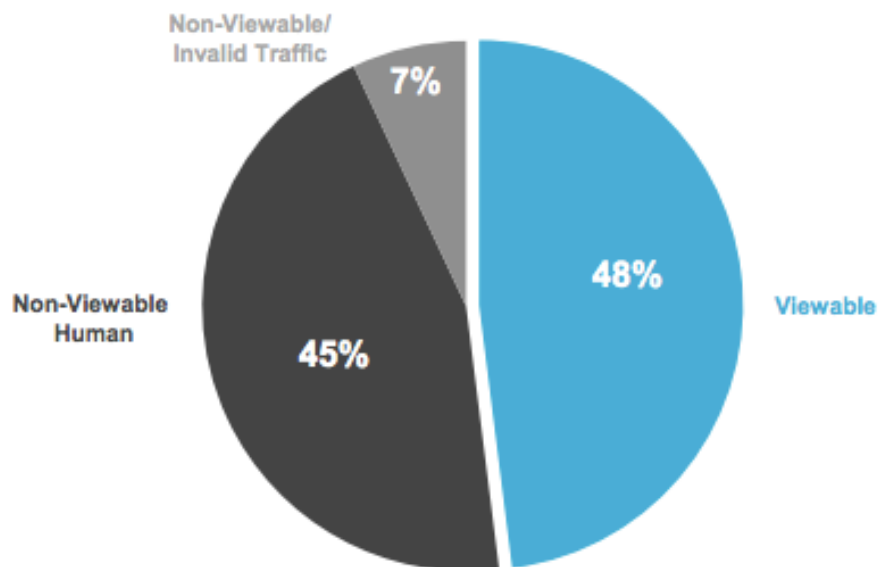
Source: Statista, 2018

Annex V – Smartphone subscriptions per region between 2014 and 2020



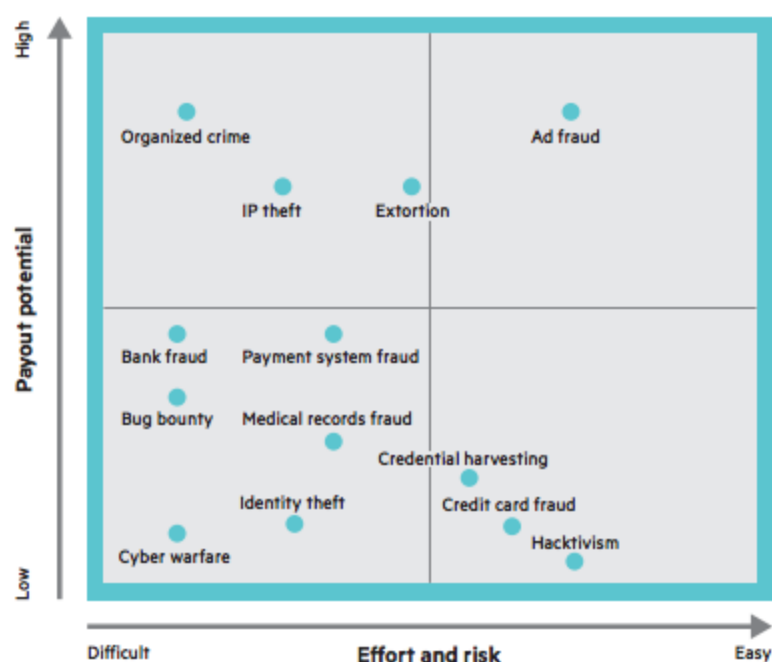
Source: Ericsson, 2015

Annex VI – Percent of U.S Digital ad impressions by viewability and non-viewability



Source: comScore, 2016

Annex VII – Attractiveness of hacking based on effort and profit



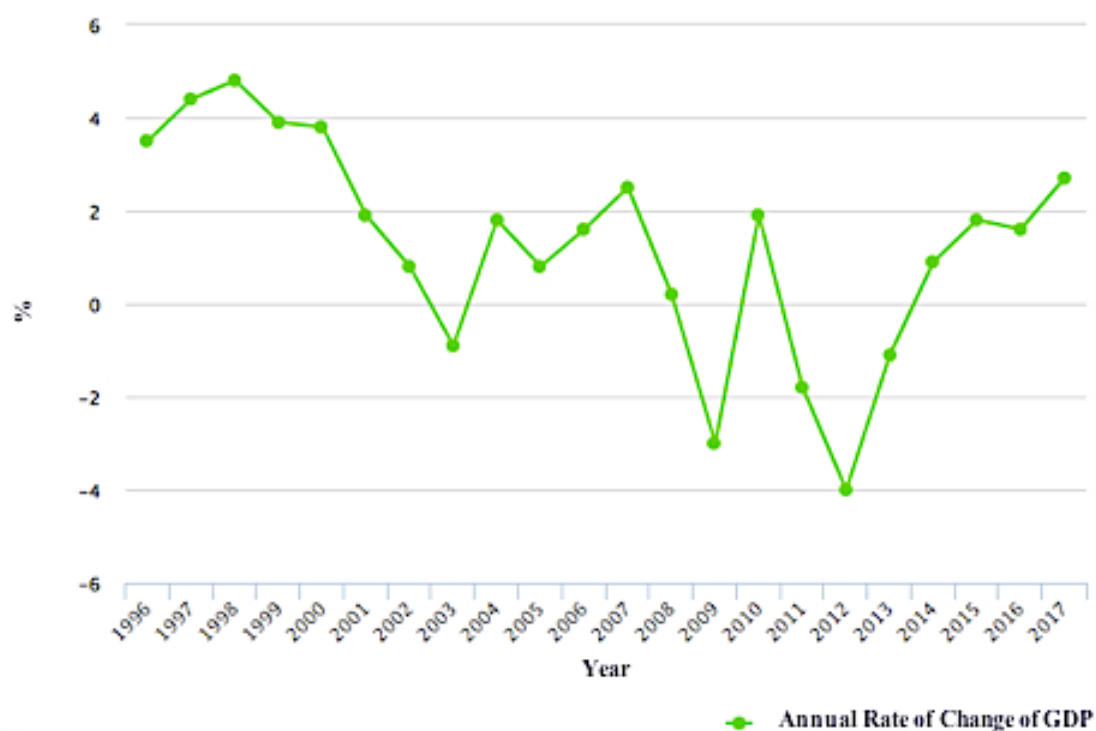
Source: Hewlett Packard, The Business of Hacking, 2016

Annex VIII – GDP growth in the EU-28 during 2006 and 2016

	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	Average 2006-2016
EU-28 (*)	3.3	3.1	0.4	-4.4	2.1	1.7	-0.5	0.2	1.6	2.2		0.7
Euro area (EA-19) (*)	3.2	3.0	0.4	-4.5	2.1	1.5	-0.9	-0.3	1.2	2.0		0.5
Belgium	2.5	3.4	0.7	-2.3	2.7	1.8	0.1	-0.1	1.6	1.5	1.2	1.1
Bulgaria	6.9	7.3	6.0	-3.6	1.3	1.9	0.0	0.9	1.3	3.6	3.4	2.2
Czech Republic	6.9	5.5	2.7	-4.8	2.3	2.0	-0.8	-0.5	2.7	4.5	2.4	1.6
Denmark	3.9	0.9	-0.5	-4.9	1.9	1.3	0.2	0.9	1.7	1.6	1.3	0.4
Germany	3.7	3.3	1.1	-5.6	4.1	3.7	0.5	0.5	1.6	1.7	1.9	1.2
Estonia	10.3	7.7	-5.4	-14.7	2.3	7.6	4.3	1.4	2.8	1.4	1.6	0.7
Ireland	5.9	3.8	-4.4	-4.6	2.0	0.0	-1.1	1.1	8.5	26.3	5.2	3.4
Greece	5.7	3.3	-0.3	-4.3	-5.5	-9.1	-7.3	-3.2	0.4	-0.2	0.0	-2.7
Spain	4.2	3.8	1.1	-3.6	0.0	-1.0	-2.9	-1.7	1.4	3.2	3.2	0.3
France	2.4	2.4	0.2	-2.9	2.0	2.1	0.2	0.6	0.9	1.1	1.2	0.8
Croatia	4.8	5.2	2.1	-7.4	-1.7	-0.3	-2.2	-1.1	-0.5	1.6	2.9	-0.2
Italy	2.0	1.5	-1.1	-5.5	1.7	0.6	-2.8	-1.7	0.1	0.8	0.9	-0.6
Cyprus	4.5	4.8	3.9	-1.8	1.3	0.3	-3.2	-6.0	-1.5	1.7	2.8	0.2
Latvia	11.9	9.9	-3.6	-14.3	-3.8	6.4	4.0	2.6	2.1	2.7	2.0	0.6
Lithuania	7.4	11.1	2.6	-14.8	1.6	6.0	3.8	3.5	3.5	1.8	2.3	1.9
Luxembourg	5.2	8.4	-1.3	-4.4	4.9	2.5	-0.4	4.0	5.6	4.0	4.2	2.7
Hungary	3.9	0.4	0.9	-6.6	0.7	1.7	-1.6	2.1	4.0	3.1	2.0	0.6
Malta	1.8	4.0	3.3	-2.5	3.5	1.4	2.6	4.5	8.3	7.4	5.0	3.7
Netherlands	3.5	3.7	1.7	-3.8	1.4	1.7	-1.1	-0.2	1.4	2.0	2.2	0.9
Austria	3.4	3.6	1.5	-3.8	1.9	2.8	0.7	0.1	0.6	1.0	1.5	1.0
Poland	6.2	7.0	4.2	2.8	3.6	5.0	1.6	1.4	3.3	3.8	2.7	3.5
Portugal	1.6	2.5	0.2	-3.0	1.9	-1.8	-4.0	-1.1	0.9	1.6	1.4	-0.2
Romania	8.1	6.9	8.5	-7.1	-0.8	1.1	0.6	3.5	3.1	3.9	4.8	2.4
Slovenia	5.7	6.9	3.3	-7.8	1.2	0.6	-2.7	-1.1	3.1	2.3	2.5	0.8
Slovakia	8.5	10.8	5.6	-5.4	5.0	2.8	1.7	1.5	2.6	3.8	3.3	3.1
Finland	4.1	5.2	0.7	-8.3	3.0	2.6	-1.4	-0.8	-0.6	0.3	1.4	0.1
Sweden	4.7	3.4	-0.6	-5.2	6.0	2.7	-0.3	1.2	2.6	4.1	3.2	1.7
United Kingdom	2.5	2.6	-0.6	-4.3	1.9	1.5	1.3	1.9	3.1	2.2	1.8	1.1
Iceland	5.0	9.4	1.5	-6.9	-3.6	2.0	1.2	4.4	1.9	4.1	7.2	2.0
Norway	2.4	2.9	0.4	-1.6	0.6	1.0	2.7	1.0	1.9	1.6	1.0	1.1
Switzerland (*)	4.0	4.1	2.3	-2.1	3.0	1.8	1.0	1.8	2.0	0.8		1.6
Montenegro							-2.7	3.5	1.8	3.4		
The former Yugoslav Republic of Macedonia	5.1	6.5	5.5	-0.4	3.4	2.3	-0.5	2.9	3.6	3.8	2.4	2.9
Albania (*)	5.9	6.0	7.5	3.4	3.7	2.5	1.4	1.0	1.8	2.6		3.3
Serbia	4.9	5.9	5.4	-3.1	0.6	1.4	-1.0	2.6	-1.8	0.8	2.8	1.3
Turkey (*)	7.1	5.0	0.8	-4.7	8.5	11.1	4.8	8.5	5.2	6.1		4.9
Kosovo (*)				3.6	3.3	4.4	2.8	3.4	1.2	4.1		
China (including Hong Kong) (*)	12.7	14.2	9.7	9.4	10.6	9.5	7.9	7.8	7.3	6.9		9.2
Japan	1.4	1.7	-1.1	-5.4	4.2	-0.1	1.5	2.0	0.3	1.2	1.0	0.5
United States	2.7	1.8	-0.3	-2.8	2.5	1.6	2.2	1.7	2.4	2.6	1.6	1.3

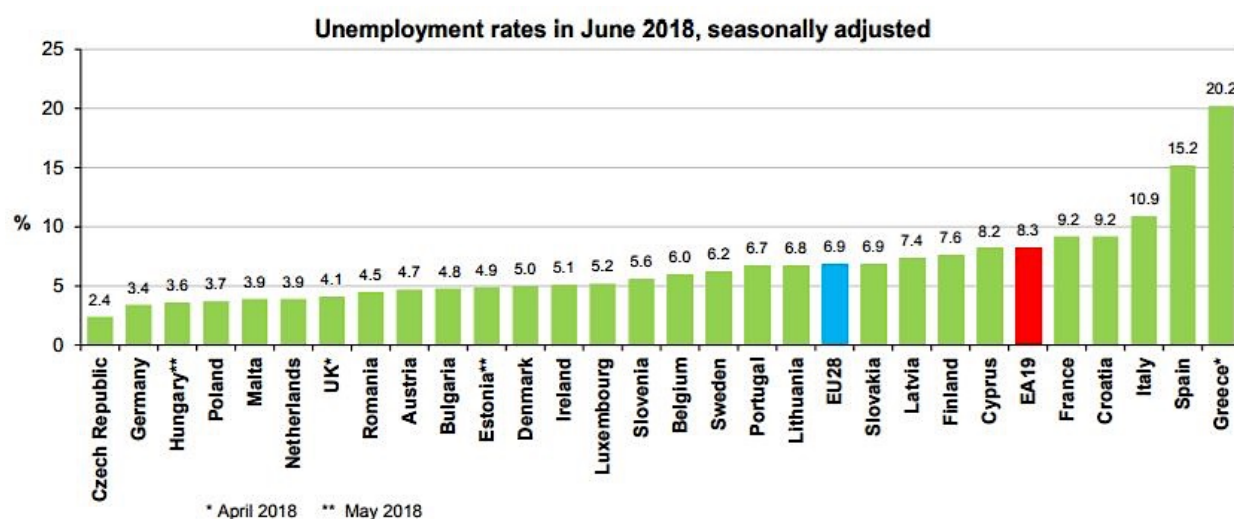
Source: Eurostat, 2017

Annex IX – GDP evolution between 1996 and 2017



Source: INE, 2017

Annex X – Unemployment rate in member states of the European Union in June 2018 (seasonally adjusted)



Source: Eurostat, 2018

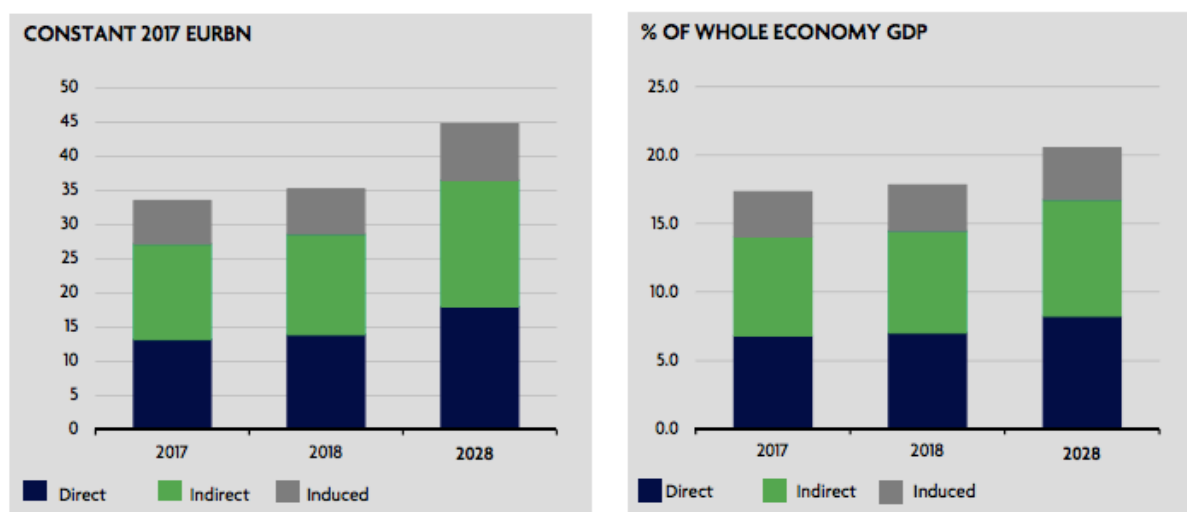
Annex XI – EU-28 Construction, annual rate of change 2005-2017

	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017
EU-28	1.7	3.8	3.4	-1.9	-7.7	-2.3	-0.1	-5.5	-1.7	2.7	1.1	2.5	3.8
EA-19	2.1	3.5	3.0	-2.8	-6.5	-5.2	-1.4	-5.3	-2.3	0.6	-0.7	2.6	2.6
Belgium	0.5	3.7	2.0	0.8	-3.2	-1.7	5.3	-0.9	-2.2	-0.7	-2.4	0.3	0.7
Bulgaria	31.8	24.1	27.4	12.3	-14.4	-14.7	-12.8	-1.2	-3.4	6.8	11.1	-16.3	4.7
Czech Republic	5.2	6.3	7.1	-0.2	-0.9	-7.6	-3.4	-7.3	-6.8	4.2	7.0	-5.8	3.5
Denmark	5.5	6.0	2.6	-0.1	-11.5	-6.4	3.3	0.8	-0.5	4.4	4.4	4.6	4.3
Germany	-5.3	6.1	2.9	-0.3	-0.1	-0.9	7.3	0.0	-0.1	2.9	-2.2	5.6	3.2
Estonia	22.3	26.9	13.6	-13.1	-29.9	-8.6	27.3	16.6	-0.1	-2.1	-3.5	4.6	17.7
Ireland	9.9	3.9	-13.5	-29.2	-36.9	-29.7	-16.7	-2.4	11.3	8.2	7.9	18.3	17.4
Greece	-38.8	3.3	14.3	7.8	-17.1	-29.6	-41.3	-33.5	-8.2	15.5	3.1	22.9	-14.6
Spain	10.9	2.2	-4.3	-16.3	-11.2	-20.4	-19.8	-5.4	1.5	17.4	1.7	5.1	-1.7
France	3.0	2.5	4.4	-1.9	-5.8	-2.4	-1.8	-5.1	0.6	-2.6	-2.2	-0.2	3.0
Croatia	-1.1	10.7	4.3	12.9	-5.8	-17.3	-11.3	-12.2	-4.6	-7.3	-1.0	2.4	1.5
Italy	1.0	3.8	6.4	-0.8	-11.5	-3.5	-4.4	-13.4	-10.3	-6.7	-1.9	-0.3	0.3
Cyprus	2.8	4.1	6.8	2.3	-10.6	-8.0	-6.8	-21.1	-18.9	-21.7	0.2	9.0	:
Latvia	15.2	13.3	13.7	-2.9	-34.9	-23.5	12.4	14.4	7.3	7.9	-1.2	-17.8	19.3
Lithuania	9.4	21.4	22.4	4.3	-48.3	-7.6	22.4	-7.2	11.7	16.6	-3.6	-9.6	9.6
Luxembourg	-1.0	2.3	2.8	-1.1	0.0	0.2	1.4	-3.8	-4.2	4.2	-1.5	3.7	0.4
Hungary	15.9	-0.8	-14.3	-5.1	-4.3	-10.4	-8.0	-6.6	8.5	13.6	3.0	-18.9	29.6
Malta	18.6	4.8	8.7	7.4	3.4	1.7	4.5	1.7	1.8	2.5	15.9	-3.8	13.0
Netherlands	5.1	3.3	6.2	3.9	-4.6	-10.7	0.5	-7.7	-5.1	4.2	8.2	7.0	6.5
Austria	4.9	5.9	3.9	-0.8	-1.8	-4.1	1.9	3.5	0.4	-1.7	-1.7	2.3	5.8
Poland	9.2	16.6	16.2	9.7	4.1	3.6	16.1	-5.2	-9.9	4.0	0.2	-14.5	14.2
Portugal	-1.4	-6.3	-3.8	-4.6	-10.4	-11.7	-12.7	-16.1	-16.2	-9.6	-3.1	-3.8	2.2
Romania	7.0	15.7	33.0	27.0	-15.2	-13.5	3.1	1.8	-0.7	-6.6	10.3	-4.4	-5.1
Slovenia	2.1	15.6	18.5	15.5	-21.0	-17.0	-24.8	-16.8	-2.6	19.5	-8.2	-17.7	17.7
Slovakia	14.0	15.8	5.6	11.7	-11.2	-12.0	6.0	-12.0	-5.2	-4.5	18.1	-10.9	3.6
Finland	4.4	7.7	10.9	3.3	-12.6	11.5	8.0	-0.9	-3.2	0.4	5.7	5.7	5.4
Sweden	0.0	11.5	11.4	-1.4	-12.2	8.1	2.5	-6.3	-3.3	1.0	8.0	9.3	7.5
United Kingdom	-0.5	1.4	2.3	-1.2	-11.7	7.2	2.2	-6.9	1.5	9.0	4.4	3.9	5.1
Norway	8.3	6.1	6.0	1.4	-8.7	0.0	3.0	7.5	6.3	4.6	1.5	3.6	4.4
Switzerland	3.4	3.7	0.5	2.1	0.7	1.2	2.8	-0.7	1.5	1.6	-3.8	0.1	3.2
Montenegro	5.6	42.3	1.4	19.4	-18.4	-0.3	18.3	7.8	40.0	34.9	20.3	47.7	42.0
Former Yugoslav													
Republic of Macedonia	:	:	:	20.4	7.5	16.7	28.4	8.0	43.3	-3.4	40.8	8.0	-25.9
Albania	:	:	:	:	:	:	:	:	:	:	:	:	:
Serbia	13.8	10.0	21.9	4.0	-18.3	-7.8	18.8	0.3	-20.7	2.9	21.1	7.3	6.3
Turkey	:	:	:	:	:	:	:	:	:	:	:	:	:
Bosnia and Herzegovina	:	5.4	13.0	8.8	-7.7	-12.4	-5.6	-2.9	-2.5	7.2	-3.2	-1.0	-2.3

(:) not available

Source: Eurostat, 2018

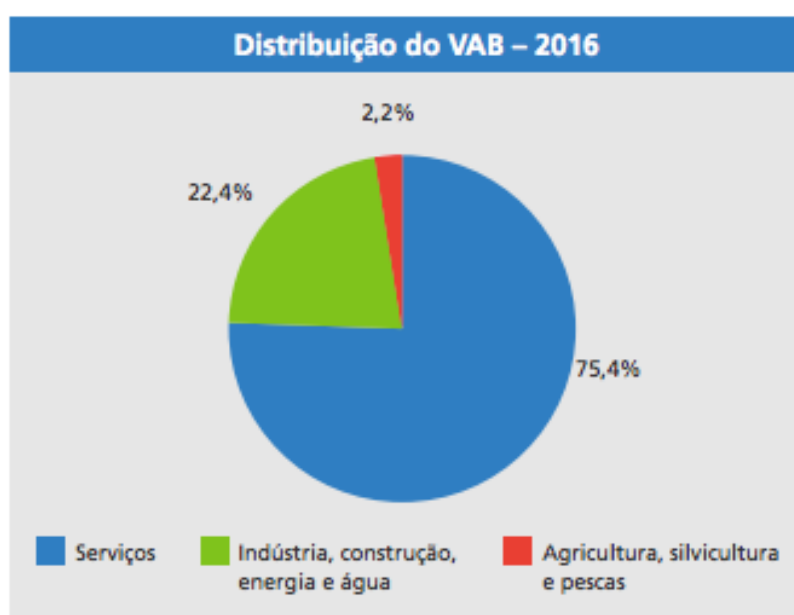
Annex XII – Total attribution of Travel and Tourism to Portugal GDP



¹ All values are in constant 2017 prices & exchange rates

Source: World Travel & Tourism Council, 2018

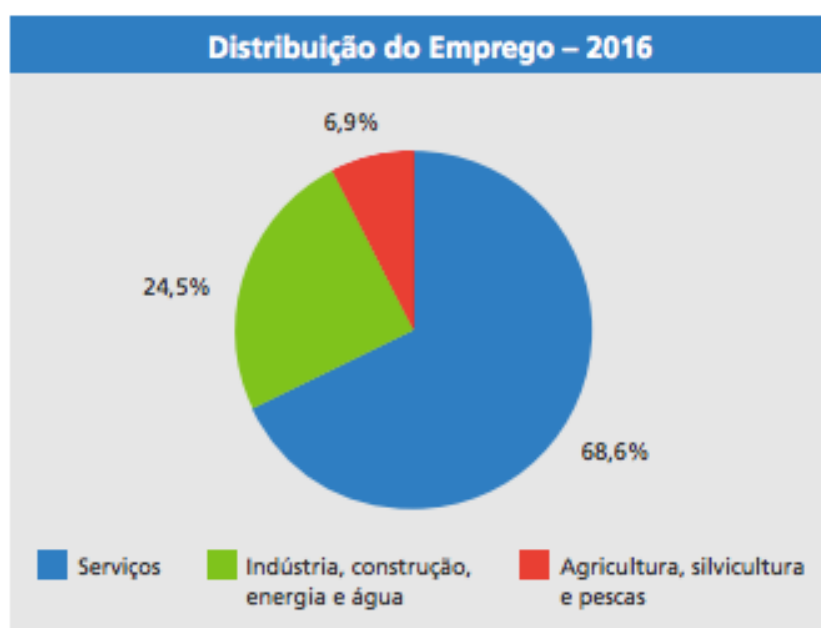
Annex XIII – Portuguese GVA distribution in 2016



Fonte: INE - Instituto Nacional de Estatística
Nota: VAB - Valor acrescentado bruto

Source: AICEP (based on INE), 2017

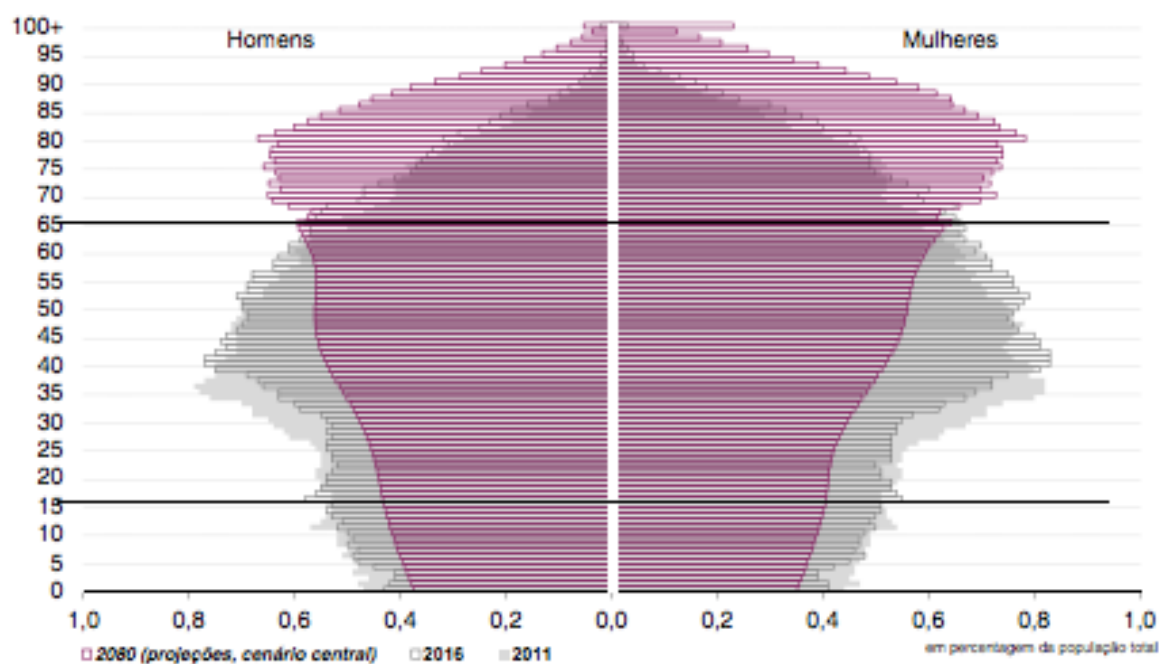
Annex XIV – Employment distribution



Fonte: INE - Instituto Nacional de Estatística

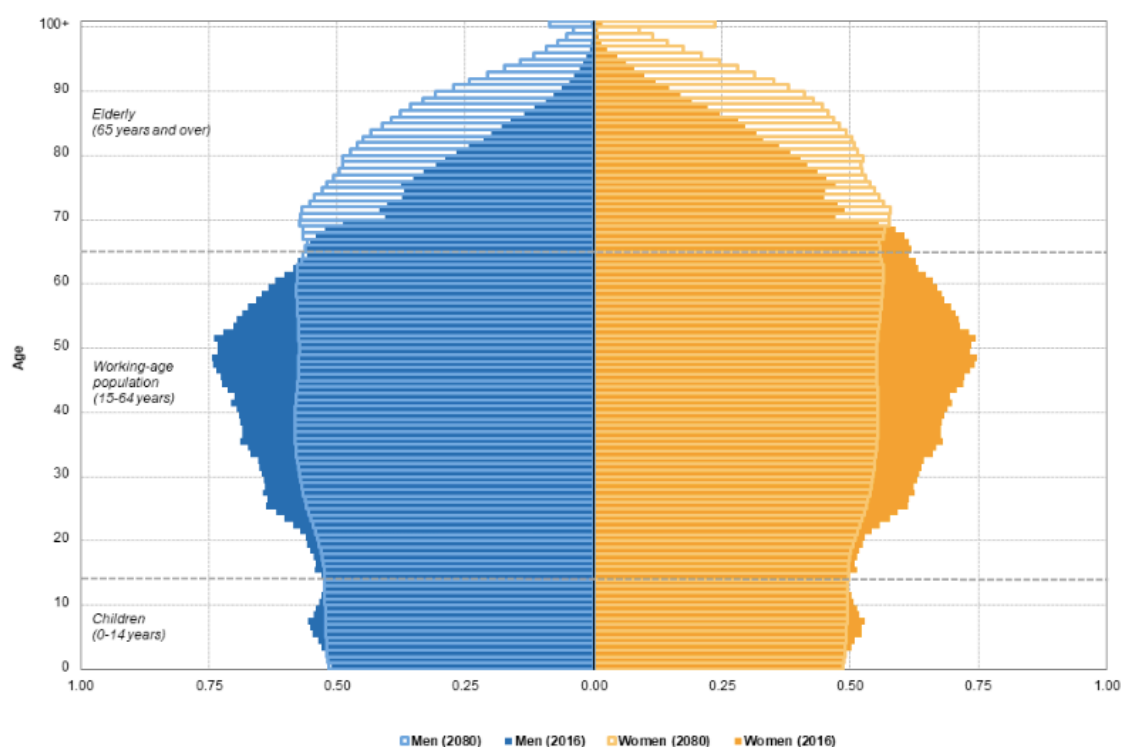
Source: AICEP (based on INE data), 2017

Annex XV – Portugal Age Pyramids 2011, 2016 and 2080 (projection)



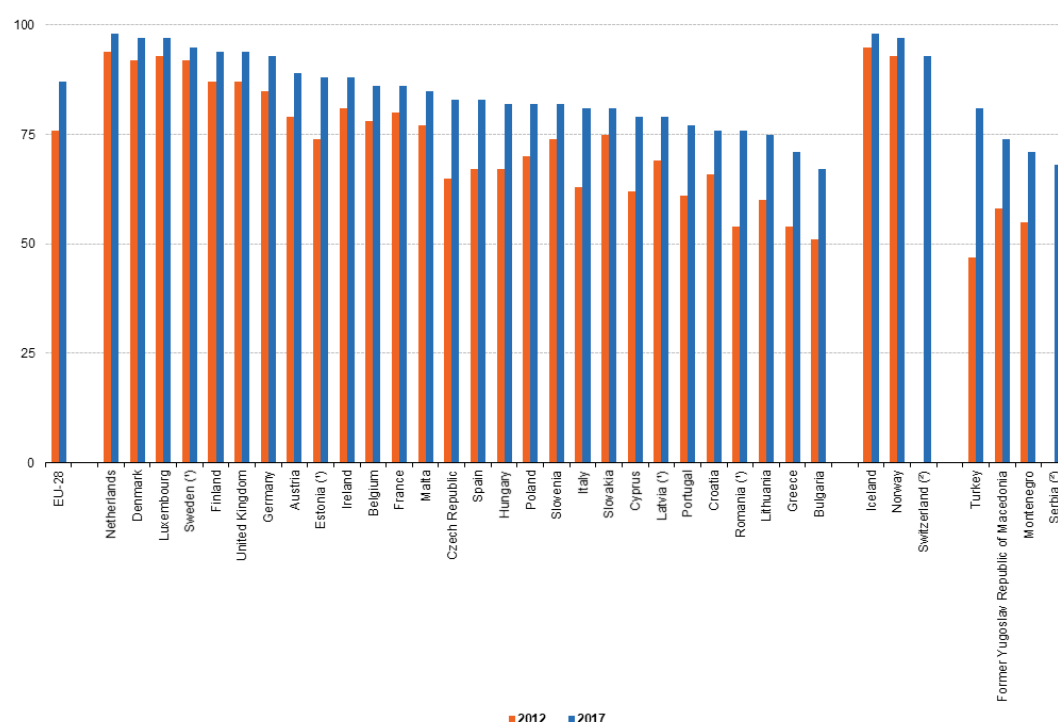
Source: INE, 2016

Annex XVI – EU-28 age pyramids, 2016 and 2080 (% of total population)



Source: Eurostat, 2017

Annex XVII – Internet Access of households between 2012 and 2017 (% of all households)



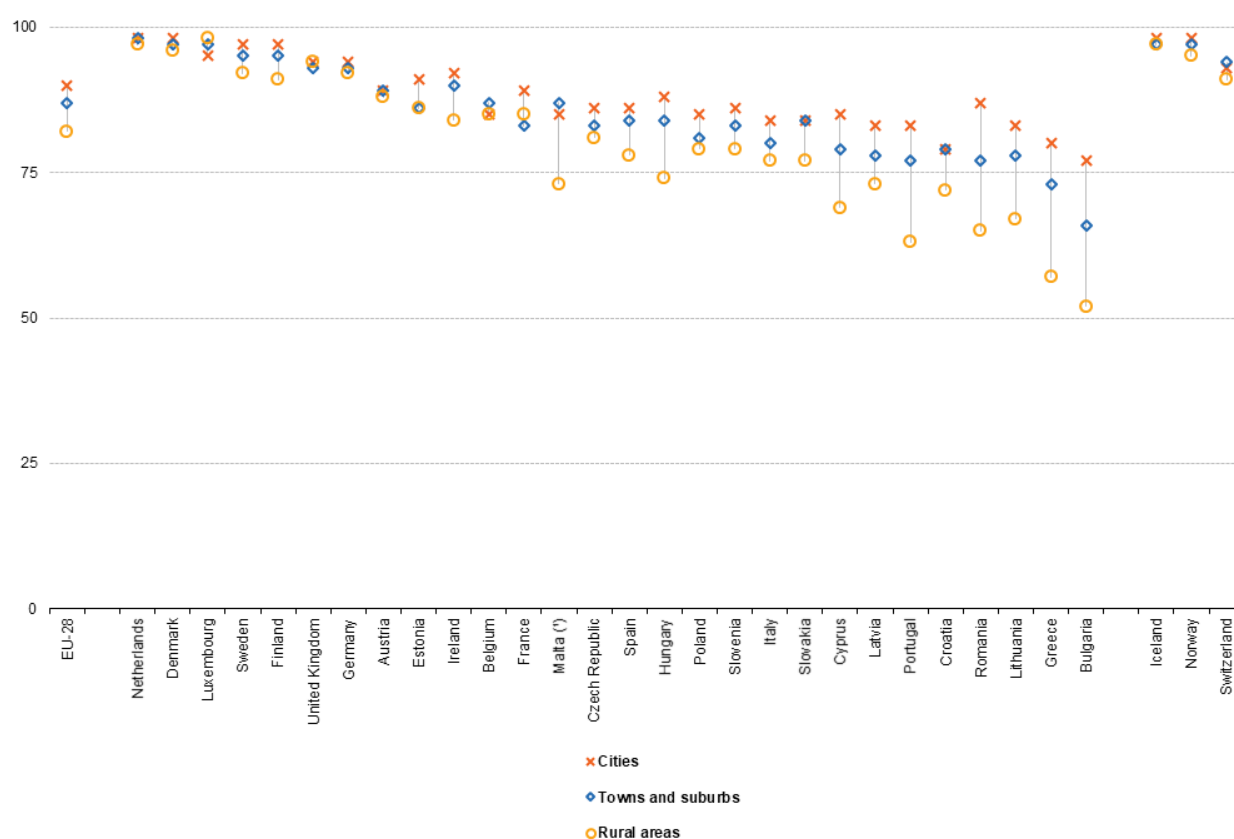
(*) Break in series.

(*) 2012: not available.

Source: Eurostat (online data code: isoc_ci_in_h)

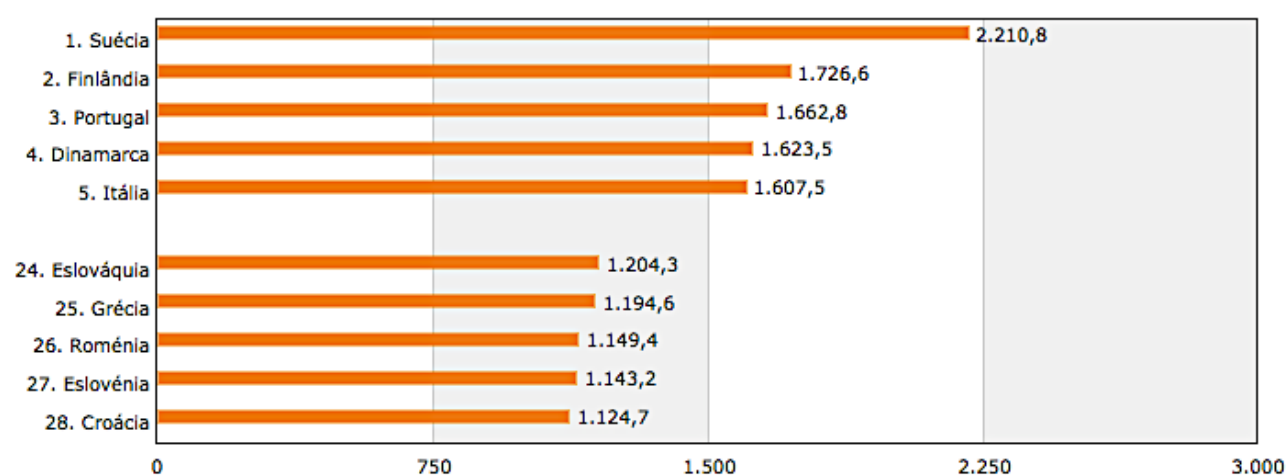
Source: Eurostat, 2018

Annex XVIII – Internet access in households by degree of urbanisation, 2017



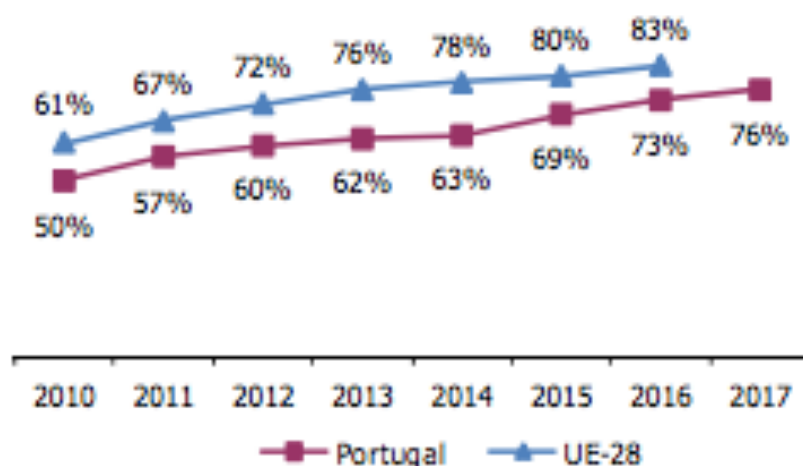
Source: Eurostat, 2018

Annex XIX – Subscribers of the mobile service per thousand inhabitants in 2016



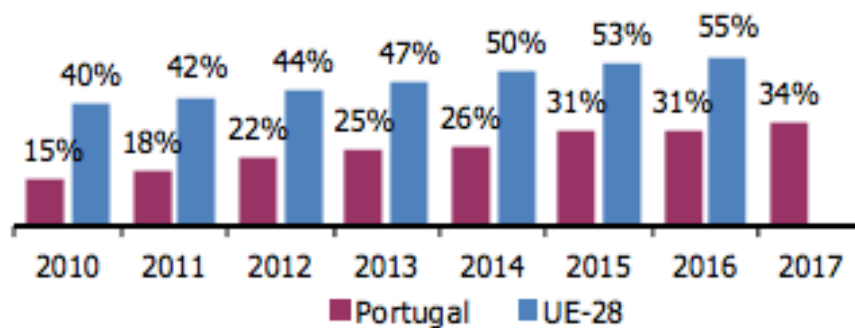
Source: PORDATA, 2016

Annex XX – Proportion of households with broadband internet at home - Portugal and EU28, 2010-2017



Source: INE, 2017

Annex XXI – Proportion of people with 16 and 74 years old using e-commerce in Portugal and EU, 2010-2017



Source: INE, 2017

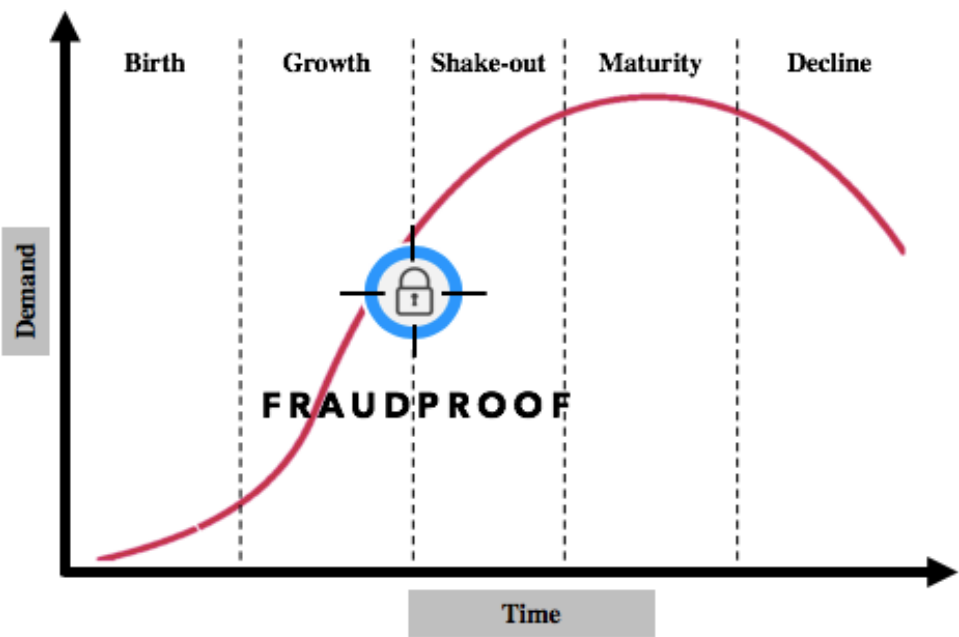
Annex XXII – 5 Forces of Porter

		1	2	3	4	5
Threat of New Entrant	Economies of scale	High	X			Low
	Products differentiation	High	X			Low
	Brand Identity	High	X			Low
	Conversion costs	High	X			Low
	Access to sales channels	Low			X	High
	Capital needs	High	X			Low
	Access to state of the art technology	Low			X	High
	Access to raw materials	Low		X		High
	Protection by government	High			X	Low
	Experience effect	High		X		Low
	Overall force value	Low		X		High
Exit barriers	Specialized assets	Low		X		High
	One-time exist costs	Low			X	High
	Strategic linkages	Low		X		High
	Emotional restraints	Low			X	High
	Legal and social restrictions	Low	X			High
	Overall force value	Low		X		High
Rivalry among competitors	Number of comparable competitors	Low	X			High
	Industry growth	High	X			Low
	Fixed or storage costs	High			X	Low
	Product characteristics	High		X		Low
	Capacity increases	Low		X		High
	Diversification of competitors	Low			X	High
	Diverse competitors (origin)	Low			X	High
	Strategic assignments	Low	X			High
	Overall force value	Low		X		High
Availability of substitution products	Availability of closely related substitution products/services	Low			X	High
	Users' conversion costs	Low		X		High
	Profitability of the substitution and product manufacturers	Low	X			High
	Aggressiveness of the substitution and product	Low			X	High

Supplier Power	manufacturers			
	Value for money of substitution products	Low	X	High
	Overall force value	Low	X	High
	Number of suppliers in the Portuguese industry	High		X Low
	Supplier concentration	Low	X	High
	Uniqueness/quality of the products/services	Low		X High
	Switching costs	Low	X	High
	Importance of volume to supplier	High		X Low
	Cost relative to total purchases in industry	Low	X	High
	Available information about suppliers	Low		X High
Buyer Power	Threat of forward integration by suppliers	Low	X	High
	Overall force value	Low	X	High
	Number of buyers in the industry	High		X Low
	Buyer concentration	Low	X	High
	Buyer volume purchases	Low	X	High
	Buyer switching costs relative to firm switching costs	High	X	Low
	Buyer profits	Low		X High
	Buyer price sensitivity	Low	X	High
	Product differences	Low		X High
	Ability to backward integration	Low	X	High
	Buyer's ability to substitute	Low	X	High
	Buyer information availability	Low		X High
	Overall force value	Low	X	High

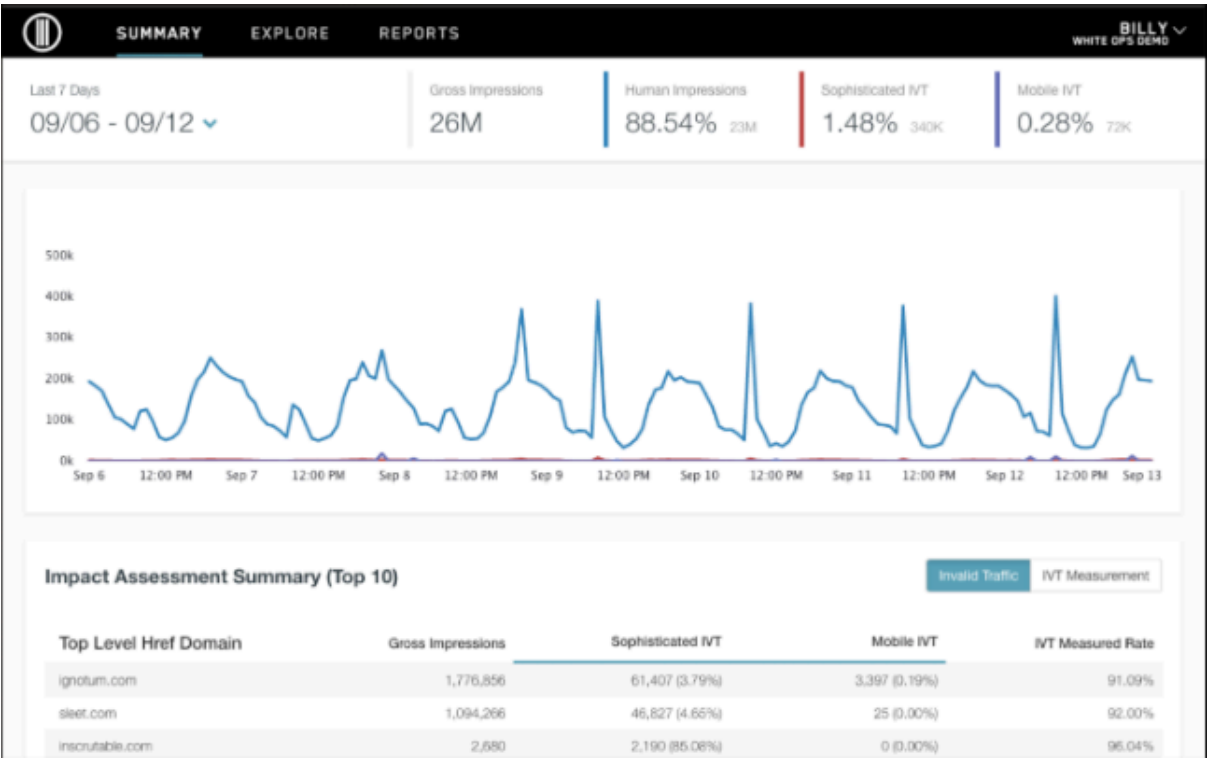
Source: The Author, 2018

Annex XXIII – FraudProof Industry Life Cycle



Source: The Author (based on Leviit, T.), 1996

Annex XXIV – White Ops FraudSensor Summary Dashboard



Source: White Ops, 2018

Annex XXV – White Ops FraudSensor Explore Dashboard

BILLY WHITE OPS DEMO

SUMMARY EXPLORE REPORTS

NEW CUSTOM VIEW **VIEWS** **FAVORITES** **RECENTS**

Campaign Invalid Traffic Summary
Campaign Invalid Traffic Summary view

Date Range: 09/06/17-09/12/17
Today Yesterday Month-To-Date **Last 7 Days** Last Month Custom

Filters

Environment
Is OR

Platform Type

Fields

Campaign ID	Environment	Gross Impressions	Decisions	Invalid Traffic (IVT)
9957325	desktop	3,393,353	2,713,641	78,876
3401243	desktop	1,802,285	1,510,805	60,901
1875061	desktop	4,402,580	4,061,553	58,104
1850617	desktop	1,278,780	1,209,167	44,006
190945	desktop	2,244,707	1,835,831	41,386
4976052	desktop	768,265	720,950	18,255
8343812	desktop	1,105,581	1,103,819	14,996
7311395	desktop	673,935	635,413	15,997
2790841	desktop	755,765	720,304	12,354
6854152	desktop	128,435	90,015	5,199
9215973	desktop	64,258	62,977	1,147
7826390	desktop	14,839	14,839	149
0	desktop	3	2	1
9957325	mobile web	378,036	364,034	1,492
Total		25,246,730	22,752,949	368,473

Showing 24 of 24 rows

*Mobile IVT is currently undergoing audit by the MPRC, and therefore, does not currently hold MPRC accreditation.

Source: White Ops, 2018

Annex XXVI – White Ops FraudSensor Reports Dashboard

BILLY WHITE OPS DEMO

SUMMARY EXPLORE REPORTS

New Report **Files** **Schedules**

WhiteOpsDemo_Provider_by_Campaign_by_Placement_ID_20170906-20170906_01-57-28_P

NAME

Provider by Campaign by Placement ID

Provider by Placement ID - clone

Provider by Placement ID

Campaign 2447814- Monthly Report

FieldReport711

Test Weekly Lookback

Untitled Report

Colleen demo

Campaign 2447814

Colleens Report

Colleen Sample

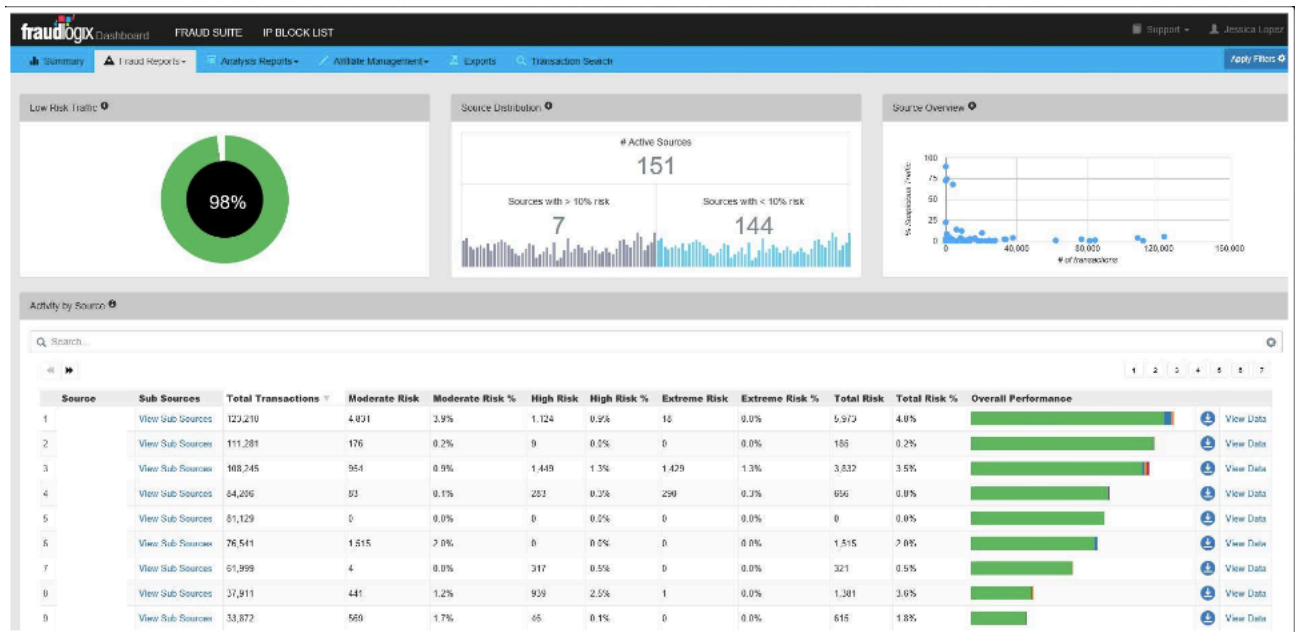
Colleen Example

These reports are not part of a regular syndicated

Campaign ID	Provider	Placement ID	Gross Impressions	Decisions	Sophisticated	Sophisticated Adware	Adware %	Pop Ups	Pop Ups %	Beta Bots	Beta Bots
3401243	beautyblog	2113179	38	38	0	0	0	0	0	0	0
3401243	beautyblog	2113179	4	4	0	0	0	0	0	0	0
3401243	beautyblog	2113179	3	3	0	0	0	0	0	0	0
3401243	beautyblog	2113179	2	2	0	0	0	0	0	0	0
3401243	beautyblog	2113179	2	2	0	0	0	0	0	0	0
3401243	beautyblog	2113179	3	3	1	0.33333333	0	0	0	0	0
3401243	beautyblog	2113179	17	16	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	1	1	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	2312	2093	34	0.01624462	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	128	122	0	0	0	0	0	0	0
3401243	beautyblog	2113179	11	8	0	0	0	0	0	0	0
3401243	beautyblog	2113179	2	2	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	2	2	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1715	1670	1085	0.6497006	0	0	0	0	0
3401243	beautyblog	2458313	4	4	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	5	3	0	0	0	0	0	0	0
3401243	beautyblog	2113179	12	11	0	0	0	0	0	0	0
3401243	beautyblog	2113179	3	3	0	0	0	0	0	0	0
3401243	beautyblog	2113179	73	69	0	0	0	0	0	0	0
3401243	beautyblog	2113179	4	4	0	0	0	0	0	0	0
3401243	beautyblog	2113179	1	1	0	0	0	0	0	0	0
3401243	beautyblog	2113179	5	4	0	0	0	0	0	0	0

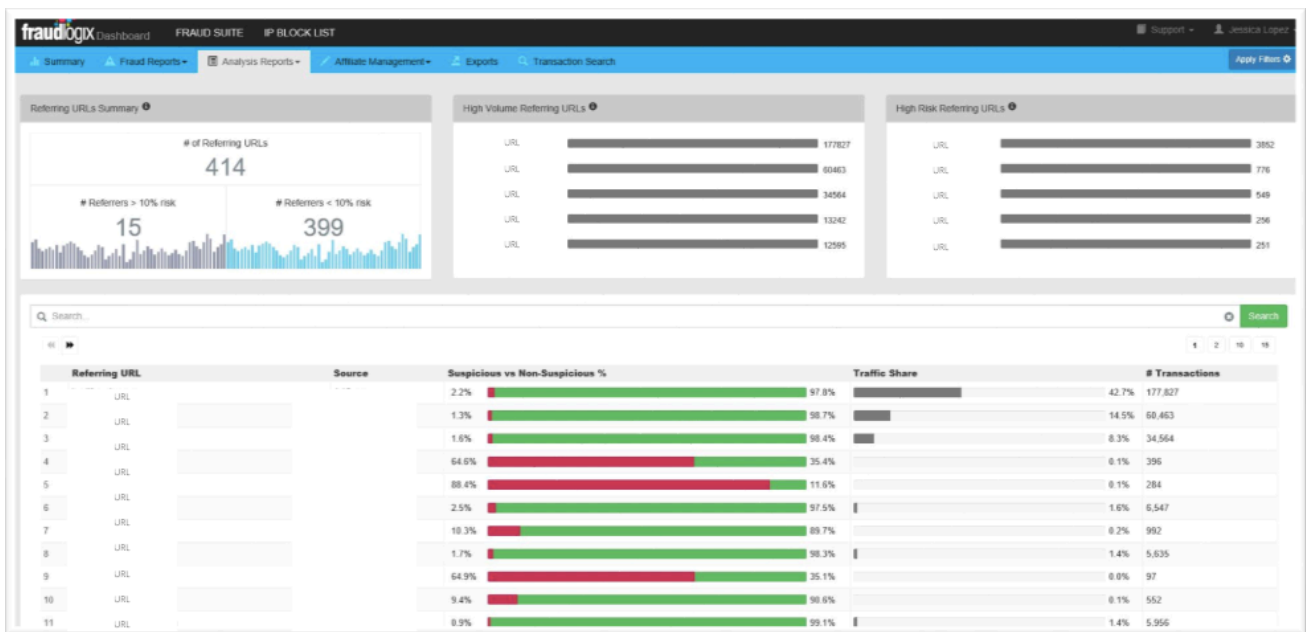
Source: White Ops, 2018

Annex XXVII – Fraudlogix Affiliate Solution Dashboard – Fraud Report



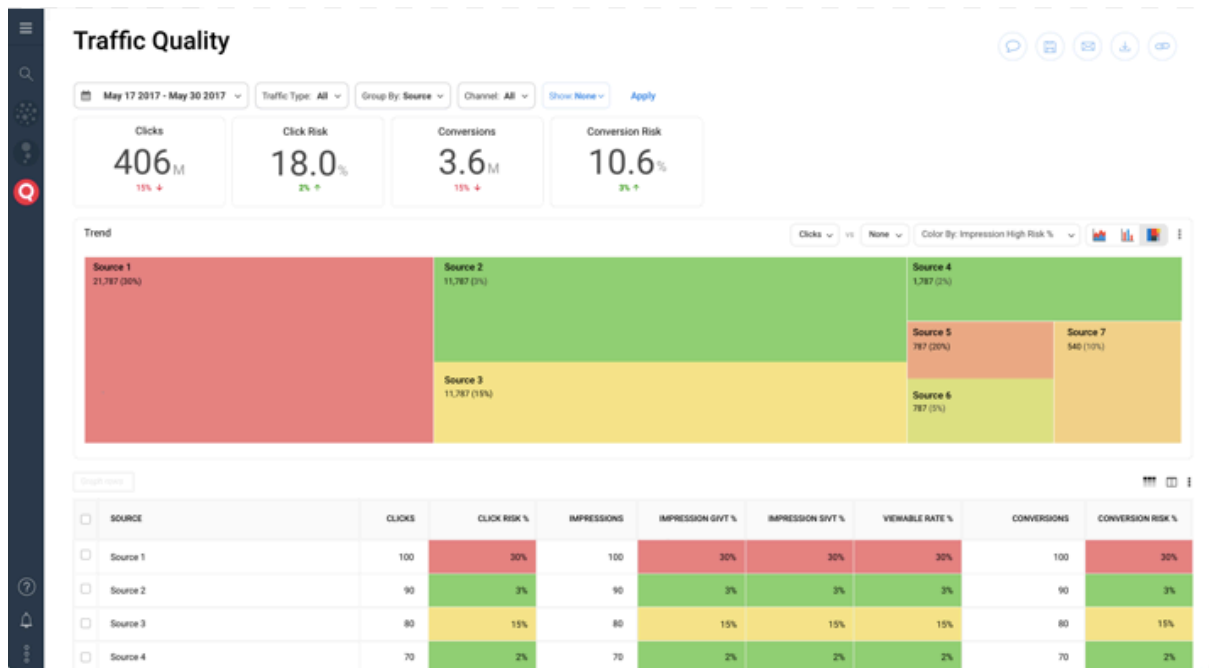
Source: Fraudlogix, 2018

Annex XXVIII – Fraudlogix Affiliate Solution Dashboard – Analysis Reports



Source: Fraudlogix, 2018

Annex XXIX – ForensIQ Ad Verification Solution Dashboard



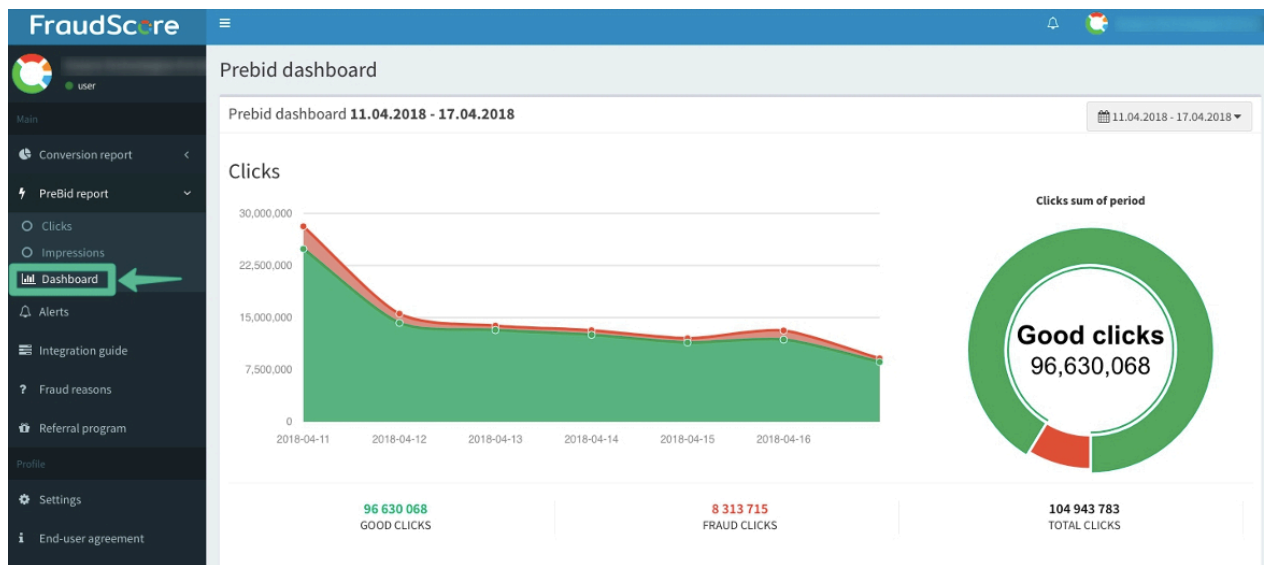
Source: Forensiq, 2018

Annex XXX – FraudScore Dashboard



Source: FraudScore, 2018

Annex XXXI – FraudScore prebid dashboard



Source: FraudScore, 2018

Annex XXXII – FraudScore Pricing Plans

STARTER	POPULAR PROFESSIONAL	ENTERPRISE	CUSTOM
\$390	\$790	\$1590	Ask
Per month	Per month	Per month	On demand
30 000 conversions included	100 000 conversions included	250 000 conversions included	Any conversions included
•\$0.02 additional conversion	•\$0.01 additional conversion	•\$0.008 additional conversion	Any volume
Support by email	Email, Skype & Live Chat Support	Email, Skype & Live Chat Support	Integrate any platform
-	Account Manager	Dedicated Account Manager	Custom functionality
-	Employee training	Employee training	
-	Sources blacklist	Sources blacklist	
-	-	Extended fraud reasons	
-	-	Smart reject	
GET FREE TRIAL	GET FREE TRIAL	GET FREE TRIAL	CONTACT US

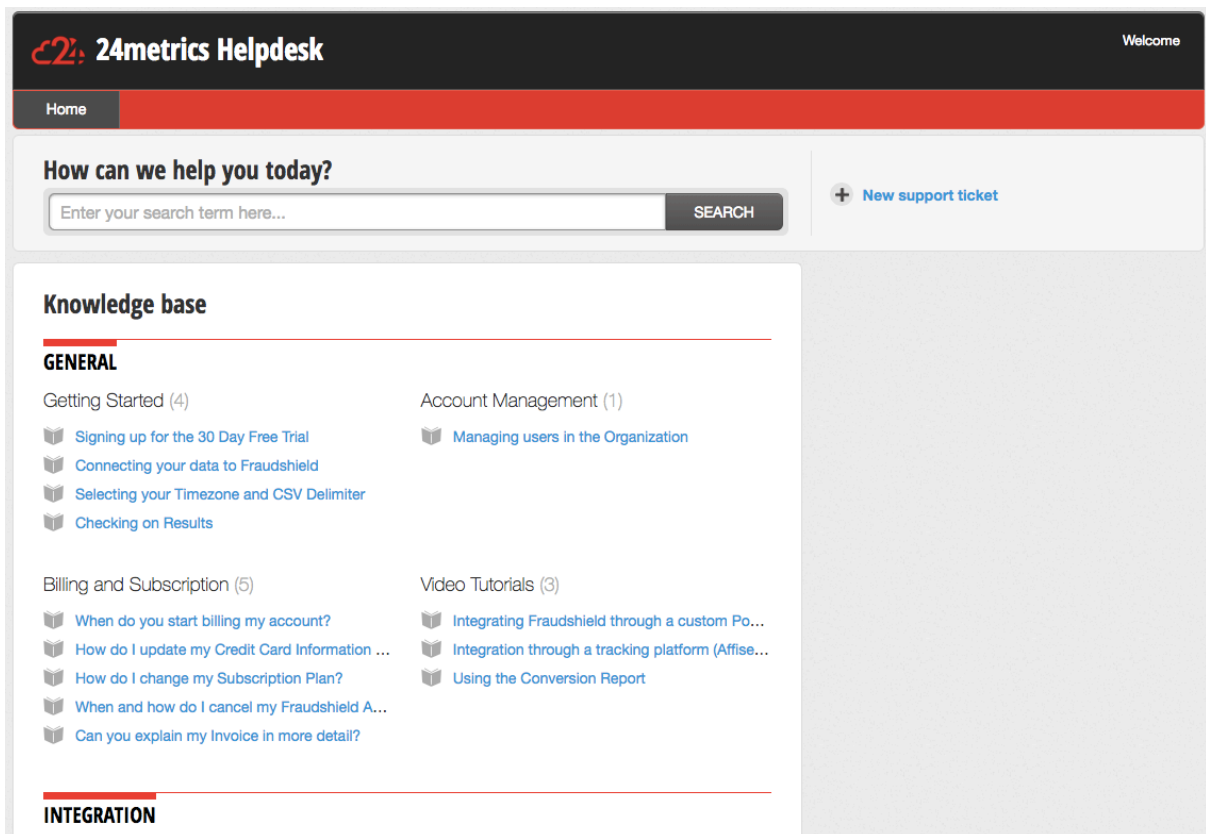
Source: FraudScore, 2018

Annex XXXIII – 24metrics dashboard



Source: 24metrics, 2017

Annex XXXIV – 24metrics helpdesk



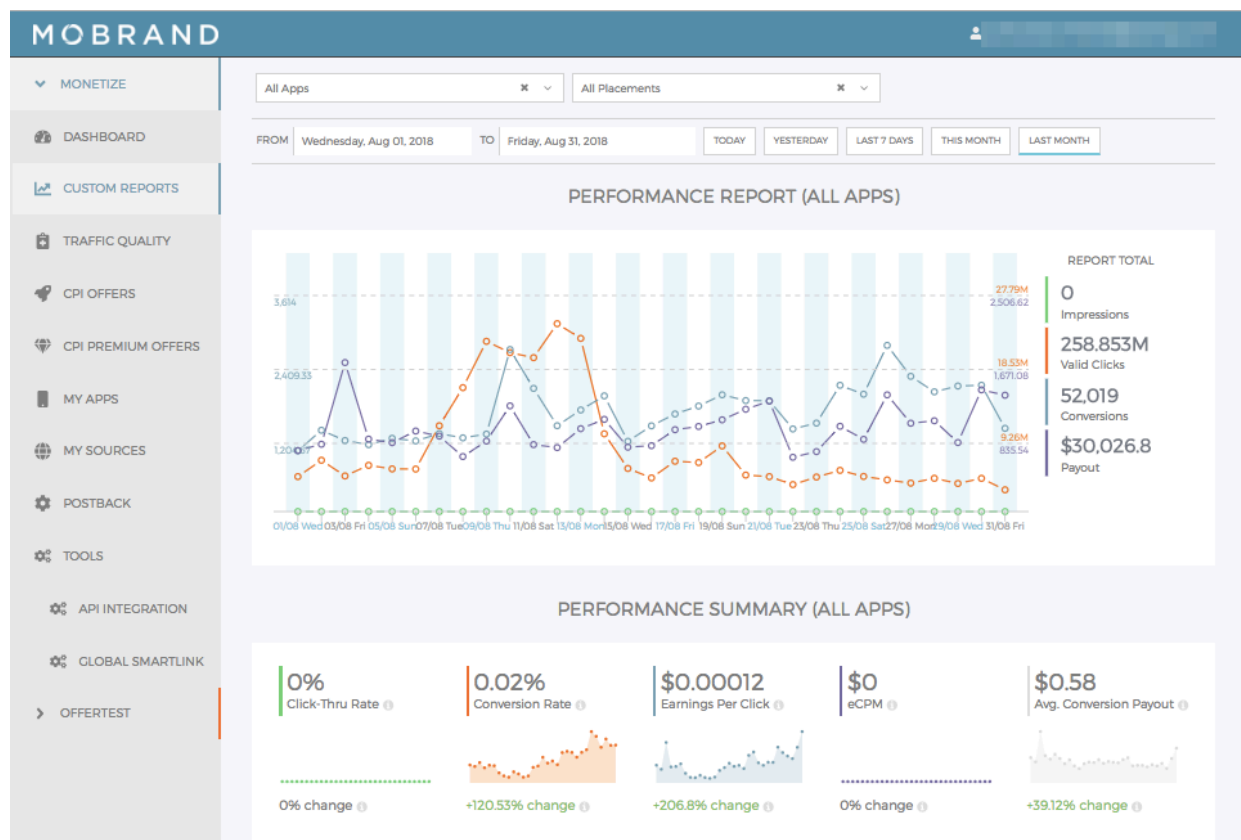
Source: 24metrics, 2018

Annex XXXV – 24metrics Pricing Plans

PROFESSIONAL	ENTERPRISE	DEDICATED	CUSTOM
Affordable Fraud Protection	Most Popular	High Volume Clients	Tailored to your Needs
\$499 per month	\$999 per month	\$1999 per month	ASK
30k conversions / mth included 0.015 USD / extra conversion 1-Click Integration - Support by email	100k conversions / mth included 0.01 USD / extra conversion - Unlimited Clicks / Goals included 1-Click Integration - Multituser Support - Support by email & phone - Account Manager - Web Training Included (2h)	250k conversions / mth included 0.0085 USD / extra conversion - Unlimited Clicks / Goals included 1-Click Integration - Multituser Support - Support by email & phone - Account Manager - Web Training Included (2h)	- Any volume - Integrate any platform - Custom functionality
START 30 DAY TRIAL NOW	START 30 DAY TRIAL NOW	START 30 DAY TRIAL NOW	LET'S TALK!

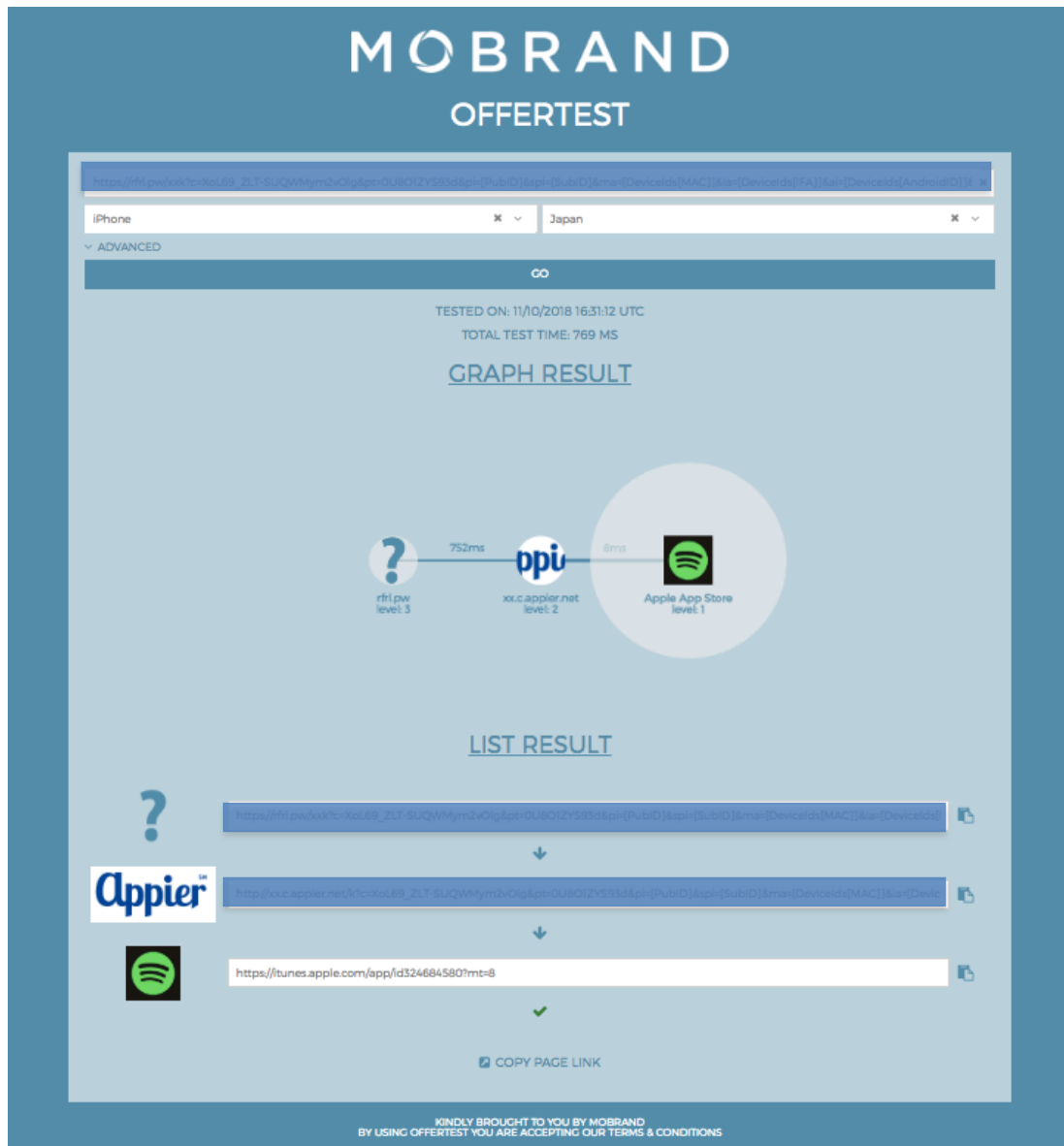
Source: 24metrics, 2018

Annex XXXVI – Console, Mobrand's Publishing Platform



Source: Mobrand, 2018

Annex XXXVII – OfferTest



Source: Mobrand, 2018

Annex XXXVIII – OfferTest pricing packages

Trial	Regular	Professional	Enterprise BEST VALUE
100K Worldwide Tests	1 Million Worldwide Tests	2,250 Million Worldwide Tests	5 Million Worldwide Tests
50 USD	500 USD	1000 USD	2000 USD

Source: Mobrand, 2018

Annex XXXIX - SWOT Analysis

Source: The Author, 2018

Strengths	Weaknesses
• Proprietary technology developed in house (OfferTest, Publisher Platform) • One stop shop for different kind of partners (small app developers to big networks/Agencies) • High quality traffic for advertisers and high quality campaigns for publishers • Low cost structure compared to other companies in the industry • Flexible operating costs due to use of external services for secondary activities (e.g. hosting on external data center) • Existent Mobrand connections with major players in the industry • Mobrand's business is boundary less, which means it cooperates at a global scale	• Mobrand's ad network image could have a negative impact in the initial launch of the anti-fraud solution as potential buyers could argue that there is an inherent conflict of interest or that it is a biased solution • Medium initial investment in development of the SaaS anti-fraud solution • Low time and HR resources availability to develop new projects; • Fluctuating demand for mobile advertising and relevant products/services associated
Opportunities	Threats
• Growth of mobile ad fraud • Mobile advertising eco-system still growing (growing number of smartphone users, mobile apps download increase) • Current and future generation are technologically savvy • Rapid technological change which motivates innovative solutions • Increased popularity of cloud based services, allowing scalability of business	• Rapid technological change • Significant global competition that offers similar services • Price wars with other players • Patent infringement/ Potential lawsuits • Existence of few specialized workforce in mobile ad fraud in Portugal, where the company is based • Increasing privacy concerns and security risk (data leakage, malware) • Changes in environment, law and regulations (i.e.: GDPRP)

Annex XL – Mobile Ad Fraud Survey

The present survey is being carried out within the master's thesis in Business Management from ISCTE Business School, and aims to evaluate the current state of mobile ad fraud and the pertinence of a SaaS anti-fraud solution for the mobile industry. The survey is intended only for mobile advertising marketers and will not take more than 7 minutes to reply.

*The answers are completely **anonymous** and **confidential**. The information will only be used for statistical purposes. Thank you in advance for your availability and participation.*

Do you work in the mobile ad industry?

- ☐ Yes
- ☐ No

If you choose “No”, please end this survey.

1. Please select the role that better represents your position in the industry.

- ☐ Advertiser
- ☐ Publisher
- ☐ Ad network
- ☐ Agency
- ☐ Other

2. What is your organization's preferred pricing model to acquire paid users?

- ☐ Cost per Thousand Impression
- ☐ Cost per Click
- ☐ Cost Per Install
- ☐ Cost Per Action
- ☐ Other (please specify).

3. What is the size of your organization?

- ☐ 0-50 employees
- ☐ 51-200 employees
- ☐ 201 -500employees;
- ☐ 501 - 1000 employees
- ☐ 1001 + employees

4. Where is your company based?

5. What are the biggest industry challenges you face today? Please rate, on a scale of 0 to 5, the importance of the following factors.

	0	1	2	3	4	5
	(Not important at all)					(Extremely important)
Privacy						
Ad fraud						
Trustworthy 3rd party measurement						
Attribution						
Brand safety						
Transparency and Trust						
Volume/Reach						
Achieving ROI (Return on Investment)						
Lack of in-app measurement						
User quality						
Other						

6. Overall, how concerned are you about ad fraud on mobile devices?

- ☐ Very concerned
- ☐ Somewhat concerned
- ☐ Not concerned

7. On a scale from 0-5, how would you rate the likelihood of mobile ad fraud increase in 2019?

0	1	2	3	4	5
(Not likely at all)					(Extremely likely)

all)	likely)
------	---------

8. On a scale from 0-5, classify the priority given by our company to mobile ad fraud prevention.

0	1	2	3	4	5
(Very Low Priority)					(Very High Priority)

9. How much of your mobile ad budget do you estimate is lost to fraud?

- ☐ Over 60%
- ☐ Between 50% to 59%
- ☐ Between 40% to 49%
- ☐ Between 30 to 39%
- ☐ Between 20% to 29%
- ☐ Less than 20%

10. What actions below do you identify as been taken by companies to tackle fraud in mobile advertising? (Please select only 3 options)

- ☐ We use fraud-related KPIs
- ☐ We analyze data to detect fraudulent patterns
- ☐ We developed internal measurement and detection tools
- ☐ We use third-party traffic validation technology
- ☐ We implemented a blacklist service
- ☐ We pay a whitelist service
- ☐ We reduce budgets assigned to mobile advertising
- ☐ We did not take any action but plan to do so soon
- ☐ We don't have plans to take any action;
- ☐ None of the above
- ☐ Other (please specify)

11. Does your company use any anti-fraud third party tool?

- ☐ Yes
- ☐ No

12. How do you expect your company dedicated fraud prevention budget to change in 2019?

- ☐ Increase

- ☐ No change
- ☐ Decrease
- ☐ Don't know

13. Please select the option below that represents best how you feel about the following statements.

	Strongly disagree	Disagree	Agree	Strongly Agree
"We have the necessary technology to detect, monitor and prevent ad fraud on a daily basis."				
"Today's fraud evolve too quickly, being hard for organizations to keep up the pace"				
"We lack knowledge about the existing types of mobile advertising fraud to successfully tackle fraud schemes"				
"We lack understanding of the types of existing solutions that fight mobile fraud types."				

14. If you could design from scratch a new anti-fraud platform, what features would it include? Please rate, on a scale of 0 to 5, the importance of the following factors.

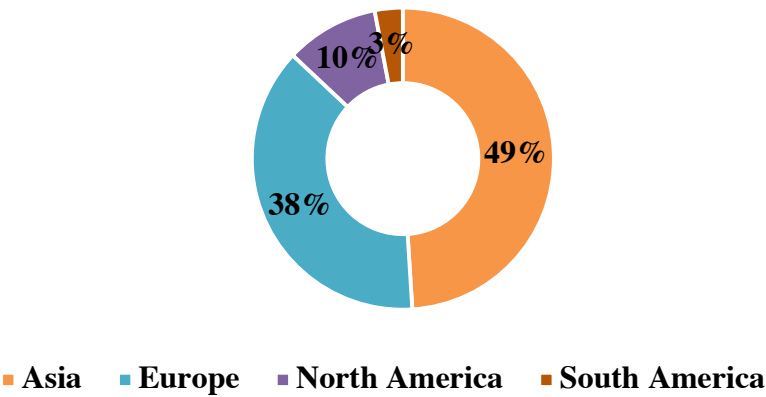
	0 (Not important at all)	1	2	3	4	5 (Extremely important)
Real-time monitoring and optimization						
Full funnel fraud detection (from click to install)						
Predictive machine-learning algorithm						
Fingerprinting technology						
Big data analytics						

Customizable Validation
Rules Setting (custom thresholds)
Inventory Scoring (SIVT/GIVT, viewability, Domain, IP, device ID)
Behavior activity detection technology (human or bot)
Proactive reject fraud conversions
Dedicated Reporting Dashboard
Extensive Exportable Reports
Fraud Analysts Team and training
Enhanced control over the account activity
Live Alerts

15. Which of the following are the most important factors in your business if you were to purchase a new anti-fraud prevention solution? (select only 3 options)

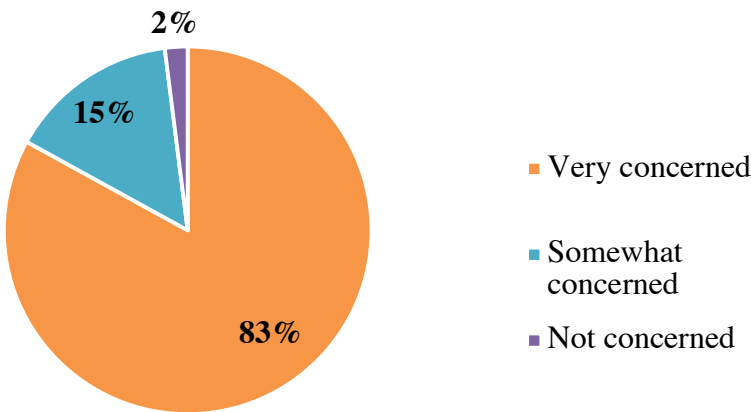
- ☐ Price
- ☐ Product Quality
- ☐ Ease of use
- ☐ Innovative features
- ☐ Compatibility with current infrastructure
- ☐ Time to implement
- ☐ Trustable brand
- ☐ Peer advice/review
- ☐ Free Trial
- ☐ Integration with trackers and marketing platforms
- ☐ Pricing plans
- ☐ Other

Annex XLI – Questionnaire Responses by continents location



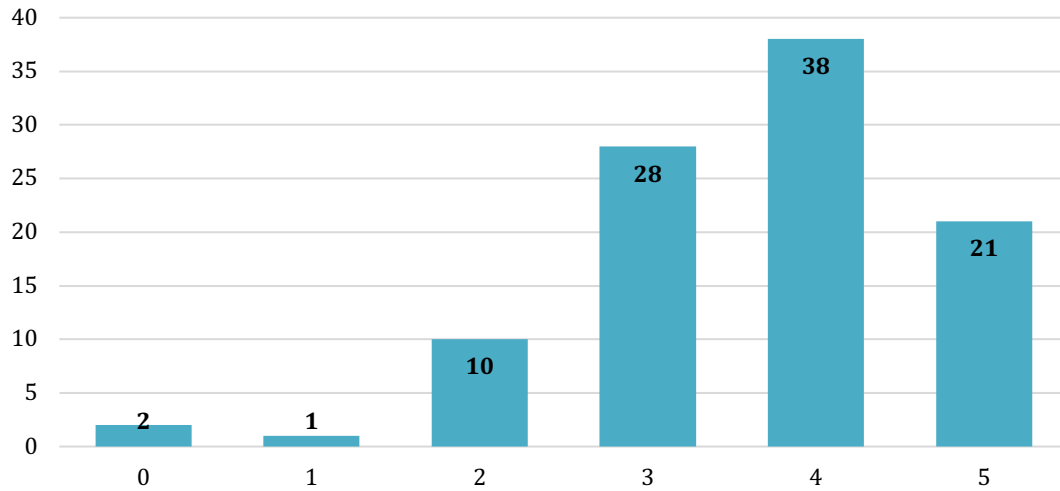
Source: Survey, 2018

Annex XLII – “Overall, how concerned are you about ad fraud on mobile devices?”



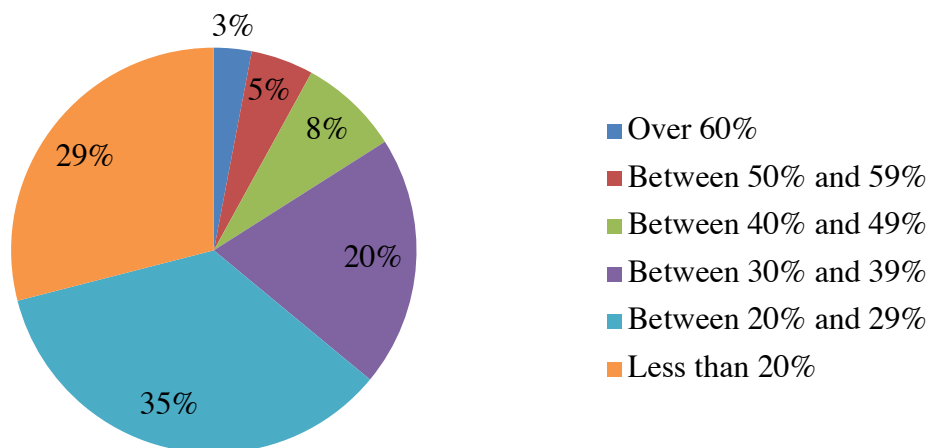
Source: Survey, 2018

Annex XLIII – “On a scale from 0-5, how would you rate the likelihood of mobile ad fraud increase in 2019? (0 being not likely at all and 5 being extremely likely)”



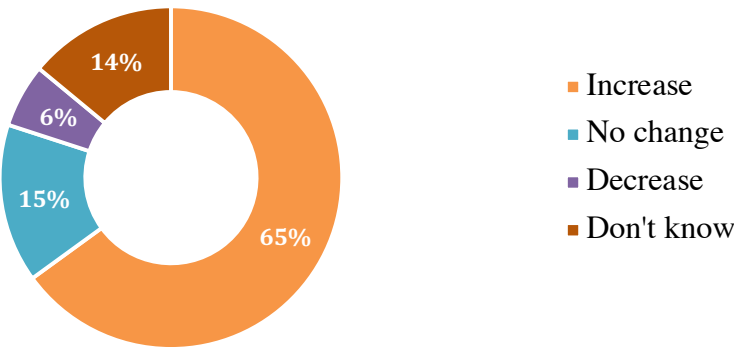
Source: Survey, 2018

Annex XLIV – “How much of your mobile ad budget do you estimate is lost to fraud?”



Source: Survey, 2018

Annex XLV –“How do you expect your company dedicated fraud prevention budget to change in 2019?”



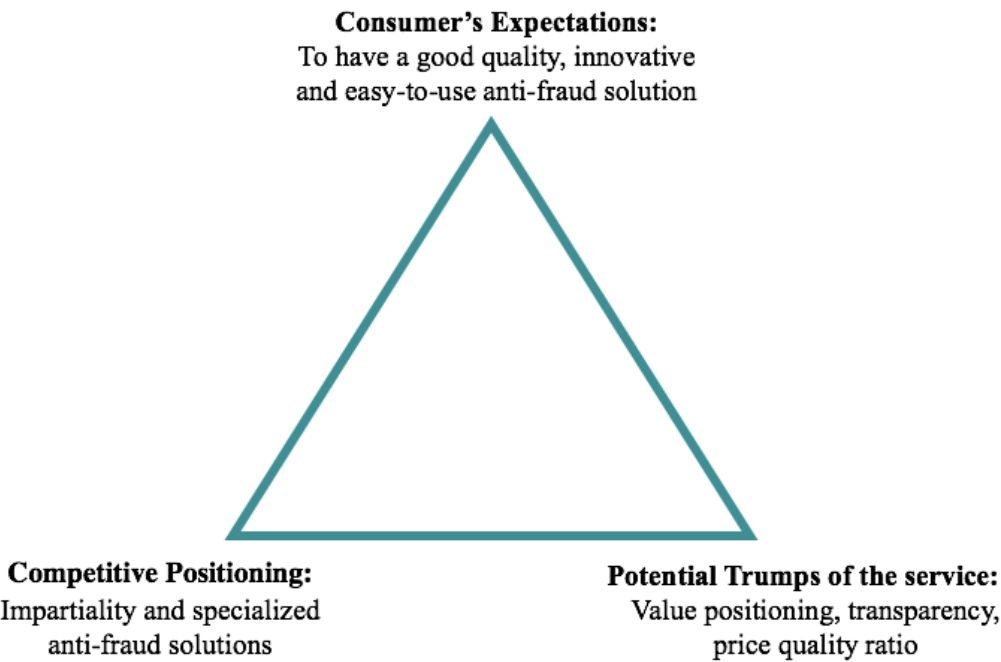
Source: Survey, 2018

Annex XLVI – Michael Porter Generic Strategies

		Competitive Scope	
		Broad Target	Narrow Target
Competitive Advantage	Costs	<u>Cost Leadership</u>	Cost Focus
	Differentiation	Differentiation Leadership	Differentiation Focus

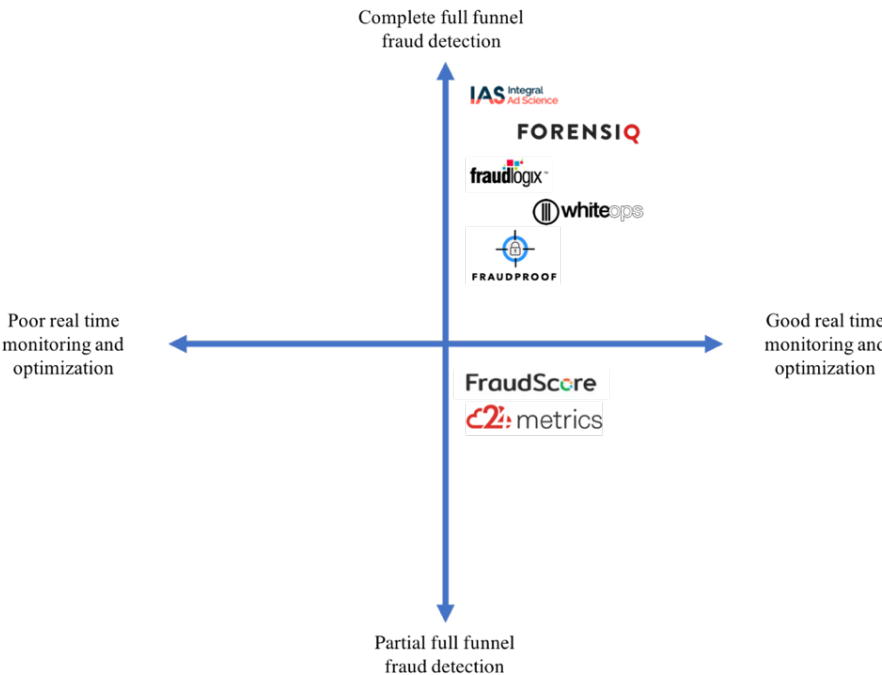
Source: Michael Porter, 1985

Annex XLVII - Golden Triangle of Positioning of FraudProof



Source: The Author, 2018 (adapted from Lindon *et al.*, 2004)

Annex XLVIII – Perceptual Map of FraudProof



Source: The Author, 2018

Annex XLIX – Official logos of FraudProof



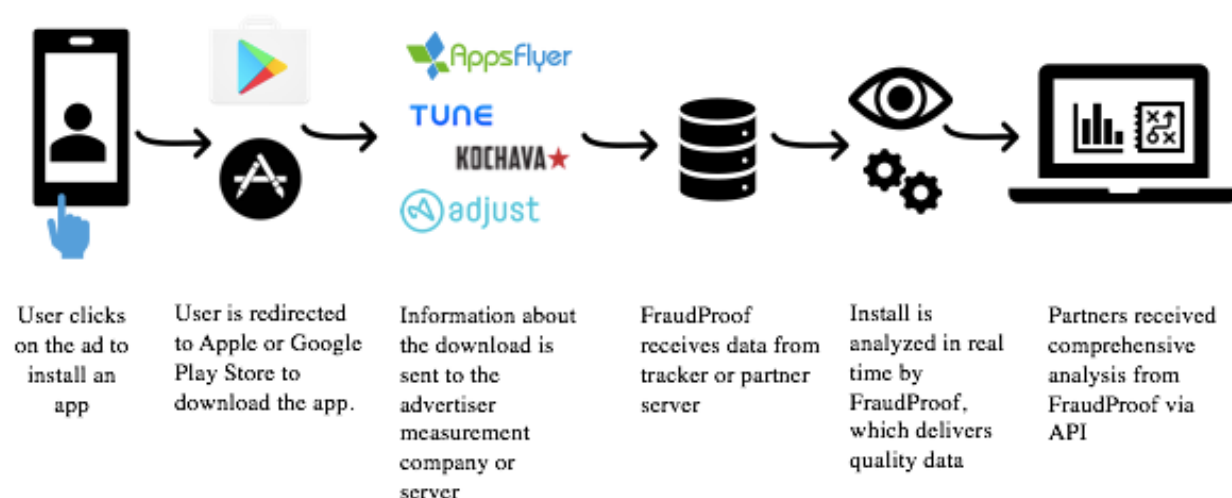
Source: The Author, 2018

Annex L – Future FraudProof Website (Landing Page)



Source: The Author, 2018

Annex LI – Information Flow of the FraudProof



Source: The Author, 2018

Annex LII – Blacklist option

Source	Campaign	Identifier/Package Name	Reason	Blacklist Date	Remove Blacklist
44579	Uber:iOS	apple.com/us/app/uber/ id368677368	Invalid Traffic	27/09/18 10:09:49 (GMT)	☐ Yes ☐ No ☐ Exception
77_974	Tinder:Android	google.com/store/apps/details? id=com.tinder	High IP repetition	03/06/18 19:22:37 (GMT)	☐ Yes ☐ No ☐ Exception

Source: The Author, 2018

Annex LIII – Reporting option

Campaign ID	Publisher ID	Source ID	Clicks	Installs	Conversion Rate	% of Duplicated IP (Conversion)	Mismatch Country-Device Language	In-App Events	Revenue
Uber:iOS	108	20_9	10000	500	5%	25%	High	n/a	\$675
Shopee:iOS	098	1_293	78690	987	1.25%	7%	n/a	n/a	\$1776.6

Source: The Author, 2018

Annex LIV – Estimated Savings Option

Source/ Campaign	Average eCPI \$1.49	Estimated Savings	Clicks			Conversions		
			Total Clicks	Total Clicks Blocked	% of Blocked Clicks	Total Conversions	Total Conversions Blocked	% of Blocked Conversions
77_974	\$1,970	\$70	2,551,559	140,578	25,5%	30,063	1,322	4,39%

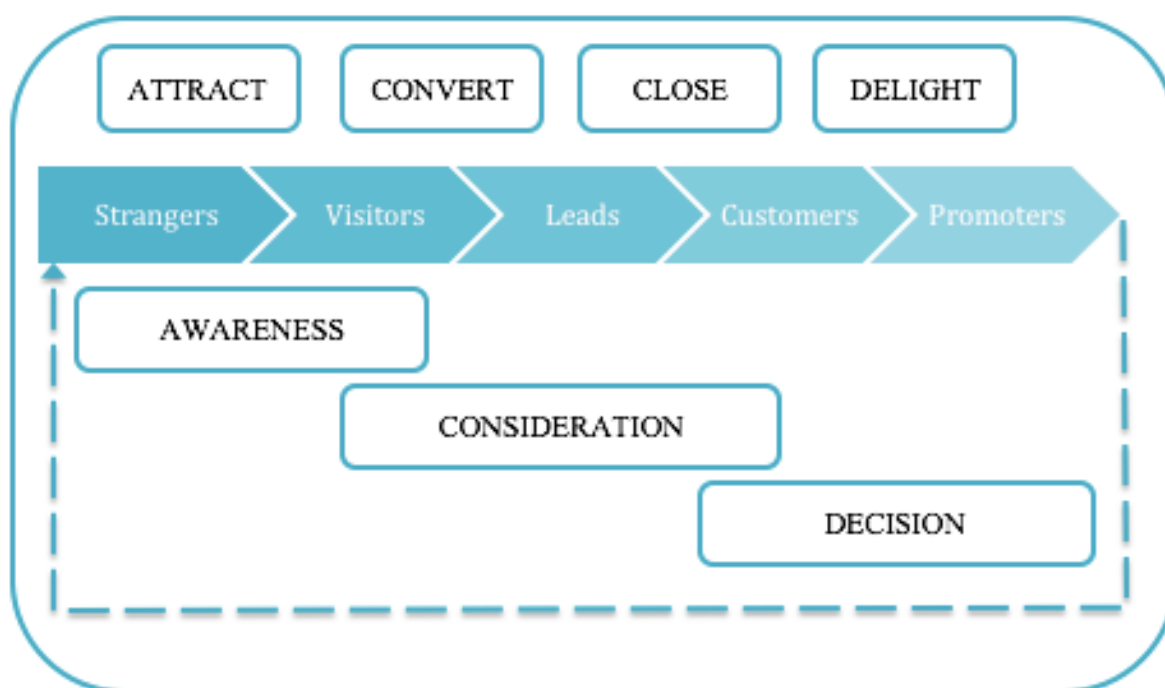
Source: The Author, 2018

Annex LV - Pricing comparison with competitors

	1 Tier Package (30,000 conversions)	2 nd Tier Package (100,000 conversions)	3 rd tier package (250,000 conversions)	4 th tier package (22 bn clicks + 425,000 Conversions)
FraudScore	\$390/month	\$790/month	\$1590/month	/
24metrics	\$499/month	\$999/month	\$1999/month	/
FraudProof	\$350/month	\$750/month	\$1550/month	\$2500/month

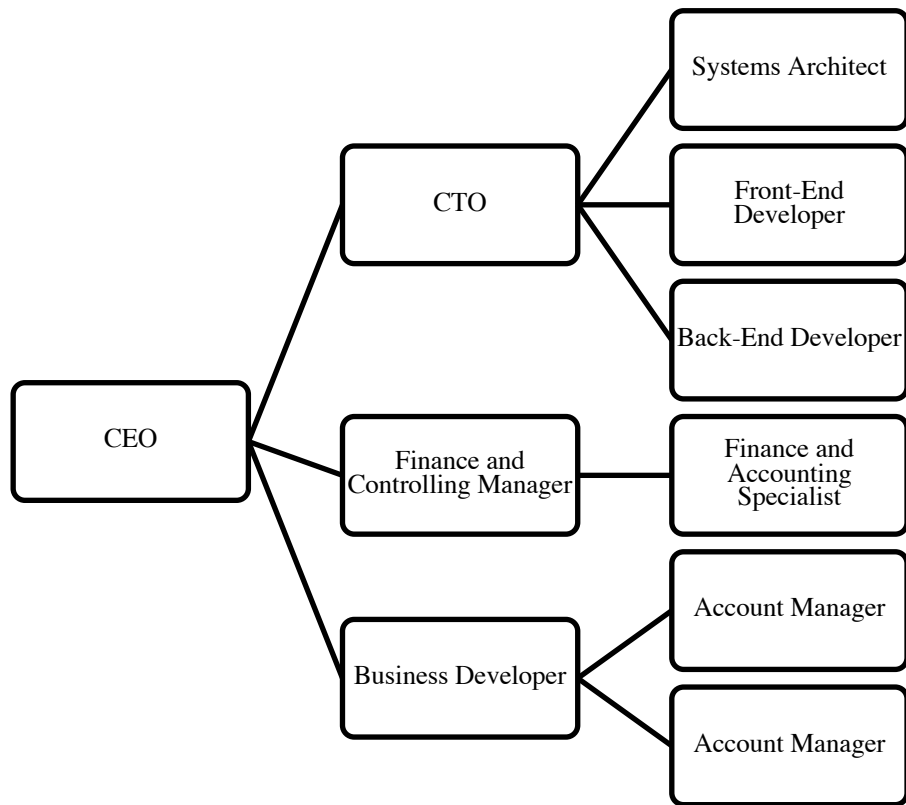
Source: The Author (Data taken from FraudScore and 24metrics Website), 2018

Annex LVI – Inbound Marketing Methodology



Source: The Author, 2018 (adapted from HubSpot, 2018)

Annex LVII – Current organization of Mobrand



Source: The Author, 2018