CATÓLICA LISBON
BUSINESS & ECONOMICS

Trust Assessment of Account Information Services Providers in Portugal: Banks, Bigtechs, and Fintechs

Nuno Vitorino

Dissertation written under the supervision of João Freire de Andrade

Dissertation submitted in partial fulfilment of requirements for the MSc in Finance, at the Universidade Católica Portuguesa, September 2020.

Acknowledgements

First of all, I could not fail to express my sincerest gratitude to Professor João Freire de Andrade for all the guidance, dedication, patience, and support throughout this process.

To my family, to whom I owe all my academic success and so much more. I am truly fortunate to be blessed with their unconditional love.

Finally, I would like to thank my friends. To all I made throughout my academic years, but particularly to those who have been encouraging and supporting me for many more years.

ABSTRACT

Account Information Services (AIS) enable users to consolidate all of their payment accounts information in a single platform. Banks, Bigtechs, and Fintechs are the main candidates to compete in the AIS market. Banks argue that consumers' trust puts them in a favourable position to dominate this market. However, since the recent global financial crisis the level of trust in banks is considered debatable. The main purpose of this research is to conclude if banks are right to hold consumers' trust as a positive differentiator from other providers. After a careful assessment of the elements determinant to the levels of trust in financial services, the usage of a primary data source allowed this research to compare different scores between institutions, not only regarding overall trust, but also in each determinant. Furthermore, this study measured the strength of the correlations between determinants and the overall institutional scores, as well as between individual's trust in the financial system and in each institution. The results showed that there is no apparent sign that banks are about to be overthrown as AIS market leaders due to the levels of trust in financial services providers. However, individuals' strong association of banks with the system, along with the highest score of Bigtechs in several determinants, and Fintechs opportunity from their image's disconnection with the system, can make the outlook change in the near future.

Title of the Thesis: Trust Assessment of Account Information Services Providers in Portugal: Banks, Bigtechs, and Fintechs

Author: Nuno Vitorino

Keywords: FinTech, Banks, Bigtechs, Fintechs, Trust, Account Information Services, Privacy, Security

Sumário

Os Serviços de Informação sobre Contas (AIS) que permitem aos usuários consolidar todas as suas informações de contas de pagamento agregadas numa plataforma. Bancos, Bigtechs e Fintechs são os principais candidatos a competir no mercado de AIS. Os bancos argumentam que a confiança dos consumidores os coloca numa posição favorável para dominar este mercado. No entanto, desde a crise financeira global, o nível de confiança nos bancos é discutível. O principal objetivo desta investigação é concluir se os bancos estão certos ao julgar a confiança dos consumidores como um fator positivo de diferenciação em relação às outras instituições. A utilização de uma fonte primária de dados permitiu que esta pesquisa comparasse diferentes pontuações entre instituições, não apenas no que se refere à confiança geral, mas também em cada determinante. Além disso, este estudo mediu a força das correlações entre os determinantes e as pontuações institucionais gerais, bem como entre a confiança do indivíduo no sistema financeiro e em cada instituição. Os resultados mostraram que não há indícios aparentes de que os bancos estejam prestes a ser derrubados como líderes do mercado AIS em Portugal devido aos níveis de confiança nos prestadores de serviços financeiros. No entanto, a forte associação dos bancos com o sistema por parte dos indivíduos, junto com a pontuação mais alta das Bigtechs em vários determinantes, e a oportunidade das Fintechs de sua desconexão de imagem com o sistema, podem fazer a mudança o paradigma em um futuro próximo.

Título da tese: Trust Assessment of Account Information Services Providers in Portugal: Banks, Bigtechs, and Fintechs

Autor: Nuno Vitorino

Palavras-chave: FinTech, Bancos, Bigtechs, Fintechs, Confiança, Serviços de Informação de Conta, Privacidade, Segurança

Table of Contents

1. Introduction

For a long time, banks have completely dominated the financial sector. However, the banking industry was not immune to the technological evolution seen in the past twenty years. The world's technological transformation is influencing consumers behaviours and preferences. They are now looking for more digital, instant, and intuitive solutions. Adding to that, there have also been important regulatory changes which ease the entrance of new players who offer innovative Fintech services. Banks are now challenged to adapt their business model to this new environment and invest in Fintech development, in order to retain their dominance of the market.

The terminology Fintech is an acronym originated by the fusion of Finance with Technology. Arner et al. (2015) defines it as the use of technology to deliver financial solutions. Correspondingly, after his extensive research on Fintech's definition, Schueffel (2016) distinguishes it as a new financial industry that applies technology to improve financial activities. Although, it is generally seen as the application of technology in the delivery of financial products, the term is also used to classify startups or companies that develop digital financial services.

Nowadays, the financial industry faces a disruptive shift brought by the revised Payment Services Directive, from this point on referred to as PSD2. Following past regulatory efforts to increase consumer choice and improving security, PSD2 focuses on increasing payment transaction and account access security, as well as the standardization of access to customer account data for different financial services providers. This new piece of legislation obligates banks to allow Third Party Providers (TPPs) access to customers bank accounts, upon their consent, in order to initiate payments or access account information, without allowing banks to receive any kind of compensation for such action.

The European Commission aimed for PSD2 to level the playing field between banks and TPPs. Financial data has turned into a commodity, forcing banks to lose an important competitive advantage. The new regulation drops barriers by giving other financial service providers access to banks client data, as well as the opportunity to better understand their needs and circumstances.

The services rising from the opening of account interfaces are Payment Initiation Services (PIS) and Account Information Services (AIS). PIS allow users to initiate a payment request online without interacting directly with their payment account provider. The PIS provider accesses the account and initiates the transaction on the payer's behalf. As for AIS, it enables users to consolidate all of their payment accounts information, from one or more institutions, giving them an overall view of their financial information.

Both PIS and AIS require the user to give out access to account data, which is extremely sensitive and private information. So, trust in the institution providing these services is a must and an extremely important influencer in users' decision-making process. AIS in particular involves sharing past transactions and balances from all the accounts. As payments turn into commodities, services like AIS become extremely valuable as they allow banks and TPPs to gather user past data and apply it in the development of other products and functionalities. Most importantly, the provider can dominate the user relationship with financial services.

Despite the adverse landscape, banks remain confident they will keep their dominant position and will be the main provider of PIS and AIS, as consumer trust in their institutions will play a major role in their favour. Furthermore, in Portugal banks are already taking steps to be ahead and benefit from the new regulatory environment, in this initial stage it is important to understand the advantages and disadvantages of the different players in the current market, and consumer trust is without a doubt a decisive one.

Therefore, this dissertation seeks to verify if banks really have consumer trust in their institutions as an advantage to exploit in the AIS market, and are in the pole position to remain the main financial data holder in Portugal. Therefore, its main goal is to compare the performance of institutions capable of providing AIS relative to Institutional Trust, and its determinants, along with perceived privacy and security. Furthermore, it is also within the scope of this research to find in each type of institution:

- Which determinants of trust are more important to explain the level of trust, on each type of AIS provider;
- The relationship of perceived privacy and security with the level of trust, on each type of AIS provider;
- The relationship between system trust and the level of trust in each type of AIS provider.

It can be divided in four main sections: The first section introduces the current regulatory framework and market ecosystem, along with its evolution until this point. The second section presents the concepts of trust (and its different dimensions), perceived privacy and security, with a particular focus on the financial services' context. The third section is where the methodology applied and the tool used (survey – Appendix A) to collect data are explained and justified. The fourth section is where the results are presented, the conclusions based on the results are discussed, as well as the limitations of this research.

In the end, this study main objective is to verify if banks are right to assume that the consumers clearly have more confidence in them as financial services providers than in the new players in the AIS market, which can be important for marketing and product segmentation decisions.

2. Literature Review

2.1. Regulatory Landscape and the Market Ecossystem

2.1.1. Regulation Overview

In early 2000s European organizations started taking steps towards a harmonized and integrated European payments market, which culminated with the Payment Services Directive in 2007. Since then, besides continuous efforts to pursue that goal, additional endeavours were incurred to adapt the market regulation to the appearance of Fintech services. Throughout the course of action to achieve that objective, each legal document had its own specific purposes but shared a common focus: regulate, secure, license, and harmonise the payment scheme in Europe, meeting consumers' needs by giving them protection and liberty of choice, thereby enhancing transparency and their control over financial data shared with TPPs.

Nonetheless, the efforts to liberalize the market started in 1992 when the signature of the Maastricht Treaty approved the creation of the European Union (EU). The agreement established the Single Market, which boosted the economic activity in Europe. It allowed free circulation between member states of goods, services, capital, and people (the accord granted EU citizenship to every person with member state citizenship). Added to the European free trade and economic cooperation zone, the Treaty set a timeline for the creation of a European Monetary Union (EMU) with a single common currency and central banking system for the EU. This materialized in the foundation of the European Central Bank (ECB) in 1998, followed by the creation of the Euro currency, that began circulating in 2002.

Since the establishment of the EMU, European authorities and institutions argued that the integration of payment systems should be a mandatory follow-up to make cross-country retail payments efficient (European Central Bank, 1999). With the intent of obligating financial institutions to self-regulate in that direction, Regulation 2560/2001 on Cross-Border Payments in Euro was adopted. It established the principle of equal-charges for cross-border and comparable domestic payments, for transactions up to €12,500.

As a result, a group of financial institutions founded the European Payments Council (EPC), which formalized a vision for Single European Payments Area (SEPA).

"*SEPA will be the area where citizens, companies and other economic actors will be able to make and receive payments in euro (...) under the same basic conditions, right and obligations, regardless of their location*" - European Payments Council: "EPC Roadmap 2004-2010".

This was the first concrete effort of European financial institutions to modernize and solidify the payments infrastructure within EU states. Banks focused in enforcing this vision on three payment instruments: credit transfers, direct debits and payment cards.

The EPC delivered as self-regulatory documents for banks the SEPA Credit Transfer Rulebook and the SEPA Cards Framework in 2008, and the SEPA Direct Debit Rulebook in 2009. While the Credit Transfer and Direct Debit Rulebooks were meant to fully replace national structures, the SEPA Cards Framework intends to mould them to better fit the new set of rules and technical standards that allowed cross-border compatibleness.

The EU appreciated EPC's work on self-regulating the sector towards achieving the vision of SEPA (European Central Bank, 2009). However, banks and other economic actors felt that it would not be possible only through private initiative for self-regulation. Specifically, it was necessary to standardize refund rules in direct debit transactions, remove balance-of-payments reporting, and institute international Bank Identifier Code (BIC) and International Bank Account Number (IBAN) to harmonize and ease payment processing (Wandhöfer, 2009). So, in order to uphold the European banking industry efforts and satisfy the need for a stronger legal basis in the implementation of SEPA, the first Payment Services Directive (PSD1) was designed.

Nonetheless, the scope of PSD1 ended up being much wider. The European Commission (2007a) set two main objectives for this directive:

"*(1) to generate more competition in payment markets by removing market entry barriers and guaranteeing fair market access and (2) to provide a simplified and fully harmonized set of rules with regard to the information requirements and the rights and obligations linked to the provision and use of payment services.*"

Therefore, the PSD1 aims at synchronizing European and national rules, as well as providing a level playing field to intensify competition amongst diverse providers by ensuring transparency and equality in the regulation (Janczuk, 2010).

PSD1 introduces TPPs to the market as Payment Institutions (PIs), intermediaries in financial transfers, and a new player in the payments market. The PSD1 was the first legal act to set an European common regulatory framework for non-bank and non-e-money payment service providers. PIs were defined as legal entities authorized to provide and execute payment services, in accordance with PSD1 regime for non-bank and non-e-money payment service providers, within the EU. This system of authorization and supervision set up by PSD1 for PIs, although similar in structure to the banking supervisory regime, was adapted to the lower risks associated with PIs, for not having permission to take deposits (Mavromati, 2008).

PSD1 also takes into account users' protection needs. The high level of consumer protection requirements was even criticized at the time for being too extensive and excessive (Wandhöfer, 2009). Besides, PSD1 gave in to banks suggestions and established the unique identifier (BIC and IBAN) and standardized the right to receive refunds in direct debit transactions.

On the same day PSD1 was transposed into national legislation (November 1, 2009) Regulation 924/2009 took effect. This act revoked Regulation 2560/2001 and substituted it as a promoter of integrated retail payment systems in the EU. Regulation 924/2009 serves as a necessary complement of PSD1 in the support of SEPA. While PSD1 standardized core payment provisions, therefore providing a favourable landscape for SEPA, Regulation 924/2009 focused on forcing compliance with SEPA Direct Debit Rulebook (which took effect one day after).

The legislation extended the principle of equal charges of cross-border and national transactions to direct debit, set a reachability requirement for payment accounts across the EU, and also controls multilateral interchange fees. These measures were meant to force banks to embrace the SEPA Direct Debit framework, as it would reduce their costs.

After several years, the European Commission (2018b) had a positive assessment over the changes brought by PSD1, and classified as its most important benefits during this period:

- Reduction of entry barriers to the market, facilitating access to new players which by its turn increased competition and choice for consumers;
- Opportunities of economies of scale, and contributed to the practical establishment of SEPA;
- More transparency to the market, and more information to consumers;
- Improved services efficiency.

Despite all the added value brought by PSD1, in 2013 the European Commission decided to revise the directive. The payment services industry was not immune to the historically fast technological development seen in the years that followed this legal act, and it resulted in the creation of more advanced services and digital solutions for which PSD1 did not account for. Furthermore, certain rules included in PSD1 were interpreted and applied differently across the member states, which led to regulatory arbitrage and legal uncertainty, especially regarding the innovations in the industry. Most of all, such environment also impacted negatively core objectives of PSD1: customer protection and balanced competition. At this point, an update in regulation was necessary.

Meanwhile, European organizations started to make efforts to solve the issues presented in the market. The European Comission's Green Paper, published in 2012, appealed for market's interest parties opinion, expectations and requirements related to the current challenges faced by the sector. The EBA's Guidelines on the security of internet payments (2014) focused on strengthened the minimum security requirements for Payment Services Providers. The aim of these initiatives was to change the market from a disintegrated and unregulated XS2A ("Access to account") standards and interfaces, to a regulatory framework suited for the present payment infrastructures (Sheja and Machielse, 2019). Following these actions, the revised Payments Service Directives (PSD2) was officially announced in 2015, publicised in the Official Journal of the European Union in 2016, and was enforced in 2019 in all member states.

2.1.2.The Revised Payment Services Directive (PSD2)

The European Commission (2018a) defined as PSD2 main objectives:

- Contribute to a more integrated and efficient European payments market;
- Level the playing field for payment service providers (especially for new players);
- Make payments safer and more secure;
- Protect consumers.

As Donnelly (2016) puts it, the update of the directive aims to expand its coverage, clarify both provider and customer's rights and obligations, as well as enhance security and authentication requirements.

In practice, PSD2 instructs banks to give access to online accessible bank accounts to TPPs for payment initiation or access account information, upon costumer consent. Furthermore, this directive clearly states that banks cannot make contractual arrangements or charge any fees for the provision of such access (Scheja and Machielse, 2019). Aforesaid changes made Hatfield (2017) classify this directive as both exciting and disruptive.

Such landscape allows for institutions other than banks (the so-called TPPs) to deepen their involvement and expand their offering in the financial services market. According to Article 4 of the directive these institutions, as well as banks, can now provide two new types of services:

- Payment Initiation Service (PIS) defined as a service to initiate a payment order at the request of the payment service user to a payment account held at another payment service provider;
- Account Information Service (AIS) defined as an online service to provide consolidated information on one or more payment accounts held by the payment service user, with either another payment service provider or with more than one payment service provider.

As such, providers of these services are called Payment Initiation Service Provider (PISP) and Account Information Service Provider (AISP), respectively.

According to the directive, PISPs act as payment initiators from the user to the merchant by creating a "software bridge" between both parties' accounts. This involves filling in the necessary information for the transfer and notify the merchant once the transaction has been initiated.

As for AISPs, these are described as providers of aggregated online information to the payment service user on one or more payment accounts held with one or more institutions and accessed via online interfaces of each payment account holder. Simply put they gather the information on the user's various bank accounts and consolidate all of it in a single place. Furthermore, the directive clearly affirms that providers of such services have as their core goal enabling the user to have an overall view of its financial situation instantly, at any given moment. In order to ensure the consumer's safety, the directive coverage must provide consumers with adequate protection for their payment and account data as well as legal certainty about the status of AISPs.

Added to these two providers, the directive distinguishes one more type: Account Servicing Payment Service Provider (ASPSP) which refers to the Payment Service Provider in which the payers' payment account is held. Therefore, its purpose is to provide and maintain a payment account for its user. As such, banks and traditional Payment Service Providers are included in this segment. These are the institutions which will be obligated to allow others (that will work as PISPs or AISPs) access to transaction and account information.

Due to the aforementioned obligation, this directive sets the use of Application Programming Interfaces as the new standard for account holders. This interface enables information exchanges between two programs without requiring both developers to reveal their complete software code (European Payments Council, 2017). The opening up of account interfaces (establishment of APIs) are the key change that unlocks the possibility of TPPs to act as PISPs and AISPs.

Another big change that comes with this new legislation refers to security measures. Colangelo and Maggiolino (2019) support the idea that this regulatory shift means that European regulators recognize the importance of Big Data in the current market landscape as well as the active role that consumers desire and should be allowed to play.
As such, the Strong Customer Authentication (SCA) brought by PSD2 boosts customer protection and security. It is translated into a two-stage authentication for online and card payments using two out of three authentication factors:

- Knowledge (e.g. PIN, Password)
- Possession (e.g. mobile phone, TAN generator)
- Inherence (e.g. fingerprint, retina)

Along with these main regulatory shifts that change the market ecosystem, in relation to PSD1 this directive adds (European Commission, 2018b):

- Includes one-leg transactions (i.e. with third countries,when only one of the parts is located within the EU);
- Updates the telecom exemption by restraining it mainly to micro-payments for digital services;
- Enhances information exchange and cooperation between authorities, in terms of
- authorization and supervision of payment institutions;
- Helps reduce charges for consumers and ban "surcharging" for card payments – a practice that is still common for online payments and in the tourism industry in some member states;
- Obligates to designate capable authorities in each member state to deal with the complaints of payment service users and other interested parties.

2.1.3. Banks and Third Party Providers in the Post-PSD2 Financial Market Landscape

In the past, the steady competitive environment, aligned with regulatory protection which raised entry barriers, put banks in a comfortable dominant position as financial services providers (Döderlein, 2018). Consequently, banks did not have to defend themselves against potential disruptive forces, and the lack of innovation characterized the sector. However, the banking industry was not immune to the technological evolution seen in the past twenty years and its effect on consumers. As stated in Roland Berger's report "Adapt or die? Why PSD2 has so far

failed to unlock the potential of Open Banking", from November 2019: PSD2 severely disrupt the business model of traditional banks, while enhancing those of TPPs. It is important to understand that TPPs are mostly Bigtechs and Fintechs.

Bigtechs refers to the internet giants, such as GAFA companies (Google, Apple, Facebook, and Amazon) and they have been slowly penetrating the European payments market since the lauch of Amazon pay in 2013. In the following year Apple launched Apple pay, and Google integrated all of its payment related services (e-wallet, as well as mobile payments and money services) in Google Pay. Their customer-centric business model joined with established brand recognition, tech resources, and gigantic research and development budgets makes them ideal candidates to take advantage of the new framework created by PSD2. According to the aforementioned report of Roland Berger, 71% of European banks see these companies as the main threat to their dominant position.

As for Fintechs, the term singles out organizations that have as sole focus use technology to deliver digital financial products and services. These companies tend to be younger and aim to provide a more specific financial service rather than a portfolio of different products. Fintechs are far from having the resources of Bigtechs but their IT infrastructure and data analysis capabilities, already suited for PSD2 shifts in the market, can make them important players in the future development of the sector. BCG's report on the digital's impact on Portuguese economy (2018) already emphasized their presence in the Portuguese banking sector:

- Revolut, a Fintech focused on giving its clients an online account that allows payments in different currencies, increased its customer-base 4.6 times to around 70 thousand users in 2018. In June 2020, Revolut already accounted for more than 500 thousand users in Portugal;
- MBWAY, developed to facilitate bank transfers and payments, accounted for an average of 2 million monthly transactions and more than 900 thousand users. In November 2019, MBWay reported more than 1 million purchases a month, with about 2 million daily users.

However, in Portugal banks seem to be ahead of the curve in the AIS market. According to Banco de Portugal, there are already several AIS options for the consumer, all of them offered by banks (September 2020). Unido, from Wizink, and Dabox from Caixa Geral de Depósitos are two examples of apps created specifically to serve the purpose of aggregating all of the

user's accounts. Apart from that, BPI, Millenium BCP, ActivoBank, BiG, and Best Bank already allow users to aggregate accounts from other banks in their apps.

Another aspect in banks favour are the requirements for TPPs to get a license to become an AIS and PIS provider, which are particularly strict in Portugal. Banks are automatically enabled to be AIS and PIS providers, as long as they fulfil all the legal requirements of the payment services and electronic money legislation. As for TPPs, besides this, they have to formally request a change of their corporate purpose, subscribe a social responsibility insurance, and get authorization from Banco de Portugal to act as AIS or PIS providers.

Despite the regulatory hardships specific to Portugal, Bigtechs and Fintechs have a very different value proposition which can be a very important factor for the consumer in his decision. On one hand, Bigtechs (such as Google, Amazon, Facebook, and Apple) have extensive tech resources as well as huge innovation budgets directed to the development of a broad range of financial services. On the other hand, Fintechs tend satisfy a specific consumer need with an innovative digital solution rather than offer a variety of financial services, which makes them competitive in their designated field, despite the much lower investment capacity. Both will definitely play an important role in the future of the PIS and AIS market, for their IT and user-centric focus which is aligned with customers' expectations.

Tied with the appearance and growing customer acceptance of Bigtechs and Fintechs as financial service providers are not only the PSD2 framework that force banks to change their business model, but also disadvantageous market conditions and regulatory requirements post-crisis, with demanding capital ratios, which can affect banks' budget and willingness to invest in innovation. Even though banks are losing some of the advantages held in the past, they are still confident in keeping their dominant position as consumer trust continues to be an extremely important advantage for them. As for the European market, in the previously mentioned Roland Berger report, representatives from more than 40 leading banks in 12 key European markets were interviewed on PSD2 impacts and effects. 54% of those banks believe the high level of consumer trust in their institutions is their main source of protection from other players. Moreover, authors that investigated impact of PSD2 tend to agree: Döderlein (2018) also praises banks reputation as trustworthy entities in assets and data management and security; Cortet at al. (2016) argues that banks are already a trusted solution while TPPs still have to keep focusing on their user-centric model to drive conversion.

Even though there appears to be a generalized idea that banks are trustworthy institutions, there is also evidence that trust in banks decreased after the 2008 financial crisis which might lead for consumers to open up for other attractive options rather than traditional banks. Several studies and reports support this idea. The PwC's Central Banking 2020 report affirms that "The crisis challenged the trust previously placed in banks. (…) To reassert their position banks need to rebuild trust and meet public expectations". Aligned with this statement, Dotti Sani and Magistro (2016) found statistical evidence that in countries such as Portugal, where the global financial crisis hit harder and the harsher austerity measures were implemented, the loss of trust in institutions was larger, especially amongst the subjects in worst economic conditions. The authors also found that the largest decline in trust in the European Parliament occurred in Portugal.

Furthermore, Fungácová et al. (2017) as well as Afandi and Habibov (2013) found statistical evidence that in countries affected by financial crisis the trust in banks is significantly lower. Fungácová et al. (2017) noted that trust in banks is lower in countries that have been affected by a financial crisis in recent years and in countries with high income per capita. The authors found that in countries suffering a financial crisis the probability of high trust decreases by 4 percentage points on average. Moreover, in the works of Afandi and Habibov (2013) there is evidence that trust in banks significantly changed from 2006 to 2010: While 47% of their sample had at least some trust in banks in 2006, in 2010 that number was reduced to 40%; Additionally, people with some or complete distrust increased from 29% to 34%.

Since trust is such an important factor in the decision-making process of consumers, and can variate over time as demonstrated above, it is important to have a complete understanding of what it is.

2.2. Trust, Perceived Privacy, and Perceived Security

2.2.1. Definitions of Trust

Trust is a complex and abstract concept. Although trust has been studied for quite some time, there is no completely accepted definition for it amongst authors, with several admitting it to be a confusing conceptualization (Shapiro, 1987; Lewis and Weigert, 1985; Barber, 1983). Rotter (1967) defined trust as an expectancy held by an individual that the word, promise, verbal, or written statement of another individual can be relied upon. In this definition's adaptation to the business environment, there are two separate elements in the customer-seller relationship that are decisive for trust to exist: the customer's expectancy of specific characteristics and behaviours of the seller, and the customer's intention to rely on the seller, based on those expectations. From that point on, the way researchers approach the concept of trust was more aligned and structured.

The majority of authors agree that trust can be interpreted as a relationship variable which implies future expectations, and some degree of vulnerability between the parts involved (Moorman et al., 1993; Morgan and Hunt, 1994; Sheppard and Sherman, 1998; Garbarino and Johnson, 1999; Grayson et al., 2008). Sheppard and Sherman (1998) view of the concept of trust summarizes and relates the most recurrent points and key aspects from the many different approaches to conceptualize trust. Trust depends on interdependence between actors and the existence of risk – If the parties involved are not somehow dependent on each other or the outcome of their actions is certain there is no need to trust. Since interdependence and risk imply vulnerability, trust is associated with vulnerability. Therefore, trust suggests positive expectations regarding future behaviours of the other party involved, as it assumes the acceptance of vulnerability. It is highly probable that some form of trust must be a part of most relationships, as they imply some degree of uncertainty in the actions of other parts involved.

Furthermore, other authors who studied trust in the specific setting of the financial and banking sector agree. Berry (1995) states that trust is involved in the choice and purchase of financial services, as there is a degree of risk, vulnerability and interdependence associated with those. In Ennew and Sekhon (2007) definition of trust, it is evident that the three factors associated with trust previously discussed (vulnerability, risk, and interdependence) are present: an individual's willingness to accept vulnerability on the grounds of positive expectations about

intentions or behaviour of another in a situation characterized by interdependence and risk. In this study, the authors argue that risk in financial services is associated with the consumer's lack of knowledge regarding the products specifications, as they are often not intuitive or straightforward. Vulnerability is also extremely present in the relationship of the consumer with the financial services provider, since poor performance or just a simple mistake can have a significative impact on the consumer's well-being. Lastly, the complexity of financial products means that the customer is dependent on his provider, at least for clarification and advise. The less customers know about financial services, the more dependent they are on their provider. So, as Kantsperger and Kunz (2010) argue, trust is important as it makes consumers overcome natural perceptions of uncertainty and risk, especially in the case of financial services where those are heightened by the consumers' ignorance about the products.

There is also evidence that trust can be differentiated by its reference object (Kantsperger and Kunz, 2010). Sekhon et al. (2014) refers to trustworthiness as a characteristic of the object of trust, the trustee. In this setting, trust is the consumers' willingness to depend on and cooperate with the trustee. It may be cognitive, when based on a reasonable assessment of the trustworthiness of the trustee, or affective, when based on feelings and emotions towards the trustee (for example, empathy). Thus, trust has an object: a person, a system, or an institution.

Person Trust is defined by the trust individuals have in other persons. Fukuyama (1995) found evidence that person trust differs from country to country. The author claims it is influenced not only by the culture, but also the legislation (level of bureaucracy is important) as well as the business mechanisms and costumes. Therefore, person trust can work as a good benchmark for system and institutional trust.

System Trust is also designated as broad-scope trust as it corresponds to individuals' expectations of dependability and reliability towards organizations, within a certain business type or purpose (Sirdeshmukh, 2002). For the purpose of this dissertation, system trust is defined as the expectation held by the consumer in banks and financial services in general, in a specific country (Portugal), related to these organizations' ability to fulfil promises and behave in a beneficial, or at least not damaging way for the customer (Gambetta, 1998).

As for Institutional Trust, also designated as narrow-scope trust (Sirdeshmukh, 2002), it is defined by the expectation of the customer that a specific institution (AIS providers, in the scope of this dissertation) complies with the established promises, and behaves in a beneficial, or at least not harmful way with the customer (Gambetta, 1998). Thus, it is related with the perception of benevolence and good intentions of the institution. However, the determinants of institutional trust may differ across stakeholders, such as customers and shareholders, as their objectives and expectations for the institution can be different.

Both Hansen (2012) and Van Esterik-Plasmeijer and Van Raaij (2017) who studied the presence and implications of trust in the financial and banking sector found interesting correlations related to the aforementioned objects of trust. Hansen (2012) concluded that if trust in the system is high, people also trust banks. Nonetheless, if the trust in the banking system is low, the level of trust the consumer attributes to the institution depends on his personal characteristics, such as wealth, knowledge, and past experiences. Van Esterik-Plasmeijer and Van Raaij (2017) found that Institutional, System, and Person Trust are positively correlated, which means that consumers who trust other individuals also tend to trust the system and financial institutions.

Nowadays, the possibility of commercial service institutions to build trust through a direct relationship with the customer is limited. Encounters with the service personnel are rare as they are increasingly replaced by self-service technologies. So, it makes it harder to build a personal relationship with the client (Meuter et al., 2000). Hence, these institutions, such as financial service providers, need to be aware of what determines the consumer's perception of an institution as a trustworthy entity.

2.2.2. Determinants of Trust

Almost all of the researchers who approached the concept of trust in the business context, also tried to find what are its determinants. The most used characteristics of trust in the literature are honesty, reliability, fulfilment, competence, quality, credibility, and benevolence (Kantsperger and Kunz, 2010).

As the scope of this dissertation is the assessment of trust in financial services providers, the determinants on which the focus will be on are the ones selected by Van Esterik-Plasmeijer and Van Raaij (2017) since this dissertation's research method is strongly based on their work, as discussed later. Van Raaij (2009) distinguished six determinants of trust: (1) competence, ability, expertise; (2) stability, predictability; (3) integrity, fairness, credibility, honesty, (consistency); (4) customer orientation, benevolence, concern about customers; (5) transparency, open and clear communications; and (6) value congruence, shared values.

Those six determinants were chosen based on:

- Ennew and Sekhon (2007), who recognized five determinants of trust: benevolence (customer orientation), integrity, ability/expertise (competence), shared values, and communications (transparency);
- Pirson and Malhotra (2008), who differentiated competence, integrity, and transparency, as determinants of trust;
- Schumann et al. (2010) distinguished ability (competence), benevolence (customer orientation), predictability (stability), and integrity as determinants of trust;
- And Sekhon et al (2014), who qualified competence, integrity, communications (transparency), shared values, and benevolence (customer orientation) as trust's five determinants.

2.2.2.1. Competence

Sirdeshmukh et al. (2002) singles out competence in the business context as the belief in the other party's ability to perform the job in an efficient and effective way. Adjacent to reliability and credibility (the belief in the expertise and abilities of the provider), competence is simply associated with trust by Kantsperger and Kuntz (2010) as the confidence of the consumer in the quality of the outcome.

Furthermore, Pirson and Malhotra (2008) incorporate technical and managerial capacity to provide relevant information, assist customers with their doubts and decisions, and solve problems and complaints. So, the competence of the provider is a mandatory requirement for a satisfactory service.

2.2.2.2. Stability

Van Esterik-Plasmeijer and Van Raaij (2017) include stability in their analysis as it encompasses the long-term perception of the consumer in relation to the institution. It is dependent on the strength, the size, and ultimately the predictability of the institution. The authors claim that consumers cannot assess the stability of an institution by themselves: they rely both in what appears on the media, and in the stability evaluation of the regulatory supervisors of financial institutions.

Moreover, Ennew and Sekhon (2007) argue that reputation and the image of a financial services provider is a main influencer of its perceived trustworthiness. Institutions would benefit from investing in managing both their reputation and image through internal policies and practices, as well as external communications and advertisement.

2.2.2.3. Integrity

Pirson and Malhotra (2008) encompass the honesty of the employees, compliance with rules, establishment of fair procedures and conditions, and the decent and equal treatment of customers in integrity as a requirement for trust in an institution. Likewise, Van Esterik-Plasmeijer and Van Raaij (2017) emphasize the organization's codes of self-regulation and

internal mechanisms to comply with governmental regulation and add the absence of deviant behaviours (such as corruption, bribery, and nepotism).

As such, van Esterik-Plasmeijer and van Raaij (2017) define integrity in this context as "fairness, morality, honesty, and "good character" of an institution", which is aligned with McKnight et al. (2002) classification of integrity as an ethical trait that depends on keeping commitments and not deceive the other party, in this case the costumer.

2.2.2.4. Customer orientation / Benevolence

Benevolence refers to the altruism behind the trustees motivations (Mayer et al. 1995). Both Ennew and Sekhon (2007) and Van Esterik-Plasmeijer and Van Raaij (2017) define benevolence as the concern of the institution with customer's interests and the extent to which the organization is willing to act from the customer's perspective, and not solely for self-interest. Ganesin (1994) suggests that the consumer's perspective about the benevolence of an institution is focused on the belief that the provider intents to act towards the customer's welfare in the face of new conditions, even if there is no pre-established commitment related to them.

According to McKnight et al. (2002) who classifies both integrity and benevolence (customer orientation) as ethical traits, their distinction is based on the expected action: integrity is dependent on keeping promises and not lying, whereas benevolence, as introduced before, invokes to the altruism behind the institution's genuine motivations (Mayer et al. 1995).

2.2.2.5. Transparency

Pirson and Malhotra (2008) advocate that transparency in financial services is defined by their openness and disclosure of information to customers, regarding the benefits, costs, and risks of their products and services.

By their turn, Van Esterik-Plasmeijer and Van Raaij (2017) add that transparency is relative to keeping the customers informed about potential and effective changes in conditions that may influence outcomes and, ultimately, their financial situation. The authors also argue that transparency can be harmful for the level of trust, as the more transparent an institution is, more likely it is that negative aspects of the products and services are communicated.

2.2.2.6. Value Congruence

Value congruence is the alignment of values and standards between customers and the institution (Ennew and Sekhon, 2007). For Hurley et al. (2014), value congruence is a comforting factor for customers, since all stakeholders are driven to associate with an organization that acts according to their values.

Ennew and Sekhon (2007) found evidence that value congruence is an area of weakness in the relationship of financial services providers with their customers.

2.2.3. Perceived Privacy and Security

Since electronic businesses started to emerge, researchers argue it is not only important to build trust (Hoffman, 1996; Keen, 2000) but also strengthen consumer's privacy and security perceptions (Friedman, 2000; Schneiderman, 2000). Even at that moment, Information Systems and Marketing authors exposed consumer concerns regarding the privacy of their information, and classified it as one of the most important issues in a technology based environment (Stewart and Segars, 2002; Miyazaki and Krishnamurthy, 2001).

Ying and Wu (2011) claimed that the growth of electronic databases, and the risk of mistreatment of information that comes with it, is the central threat to individual privacy in the modern age. At the time, most of the information passed to the existent databases was mostly not sensitive information, with no potential to harm the customer: it was mainly related with hobbies, personal preferences, and daily activities (Kaplan and Haenlein, 2010).

However, the continuous growth of both the electronic and online ways to serve the customer and the user acceptance of such services, in activities that involve sensitive personal information (such as financial, health, location, or personal identity), has generated a discussion around the possibility of unintended negative repercussions (Fife and Orjuela, 2012). KPMG, in its "Privacy Security Issues Hamper Wider Growth of Mobile Banking, Despite Increasing Consumer Acceptance" report from 2011, already identified the collection, transfer, and reuse of personal information, and the implied reduced control of the individual of his information after it has been given, as the central issue of the future of mobile banking.

Nowadays, the scenario is evidently different. While the internet usage continues to grow, and new mobile services continue appear, data processors have to continuously update their procedures to abide to data protection regulations. In what concerns financial services, a very important piece of legislation regarding privacy and security is given by the General Data Protection Regulation (GDPR), introduced in 2018. The core components of this legislation are transparency and user consent.

The GDPR aims at the protection of personal data, defined by the legislation as any information related to the identification of a natural person. The access to personal information of providers of financial services and products (such as those enabled by PSD2) must comply with this legislation, otherwise the non-compliant institutions are subject to heavy fines, and potential reputational damage. Under GDPR, financial institutions are not authorized to process consumer data without consent, which must be asked in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child, as stated in article 12 of the regulation. It makes it easier for consumers to know specifically where their data is being used, which enables them to raise objections. The GDPR also gives consumers the right to transfer their data from one financial services provider to another easily, in a machine-readable format.

According to EY's Payments Newsletter Volume 22 (2019), there is some uncertainty concerning the overlaps between GDPR and PSD2. As such, the article highlights the key actions financial institutions should take to comply efficiently with both legislations and act as AIS and PIS providers:

- Be extremely careful with automated decisions, particularly regarding the use of profiling (the automated processing of consumer data to identify and evaluate personal features) which is prohibited by GDPR;
- Design data protection tailed for AIS and PIS, and conduct regular data protection impact assessments, since the nature of these services requires the processing of high volumes of data;
- Be ready to give consumers information about the use of their data, for them to have a comprehensive knowledge of how their data is being processed, if they desire to do so, a right brought by the GDPR;
- Confirm that it is possible to erase all consumer data quickly, as consumers have the right to request it.

Additionally, with the evolution of security technologies as facial recognition, sensors and Near Field Communications (NFC) – which enables the instant transfer of information between devices with a single touch or approximation between them – are now part of everyday services, applications, and transactions (in financial services). Fife and Orjuela (2012) defend that innovations change privacy considerations and throughout time. Privacy threats started being discussed with the appearance of newspapers and cameras (Warren and Brandeis, 1890). It is likely that the same will happen with the appearance of new mobile apps and services from PSD2.

The common understanding of what constitutes privacy changes over time. Westin (1967) defined privacy as the capability of the individual to control the terms of how their personal information is acquired or used. According to Fife and Orjuela (2012) privacy is usually defined as the right to control access to one's person and to personal information about oneself. Hartmann (2011) adds that consent is a mandatory implication of privacy. Although definitions and constituents of privacy differ across disciplines, they are consistent in attributing the core of the concept to the individual's control over the access to his information.

The concepts of privacy and security are often confused, and there are some disagreements between authors regarding their distinction (Krumay and Oetzel, 2011). While some believe privacy is included in security (Landau, 2008), some believe security is included in privacy (Jin and Ahn, 2006), and others support the idea that they are two separate but related constructs (Bansal, 2017).

Bansal (2017) relies on an explanatory example of the relationship and the distinction between the concepts of privacy and security, which idea will be followed by this dissertation: The author presents an institution with little or no security. In such case, the institution is unable to protect the information held, which might lead to an event where the customers' private information is compromised. Yet, not even the best security controls would prevent or have any impact whatsoever on decisions regarding the collection, distribution, or usage of information. This suggests a clear distinction between privacy and security, and that security is necessary but not sufficient for institutions to keep privacy commitments.

"Security is about protection from malevolent actors who are trying to exploit information for a variety of motives including self-indulgence, revenue generation, and even espionage. Privacy is about governance and use." – Bansal (2017). pp.330

2.3. Research Hypothesis

As previously mentioned in the introduction, the main objective of this dissertation is to compare scores of institutional trust of Banks, Bigtechs, and Fintechs, as AIS providers, with its determinants, perceived privacy and security. Additionally, this work also intends to discover which determinants have an higher influence on the level of trust, the influence of perceived privacy and security in the level of trust, and the relationship of the level of institutional trust with system and person trust, for each type of institution.

In order to achieve the secondary objectives four hypotheses were formulated, based on the literature review of the determinants and dimensions of trust:

H1) The evaluation of the determinants of trust (competence, stability, integrity, customer orientation, transparency, and value congruence) are correlated with the level of institutional trust for Banks, Bigtechs, and Fintechs;

H2) The evaluations on perceived privacy and security are correlated with level of institutional trust for Banks, Bigtechs, and Fintechs;

H3) The level of system trust is correlated with level of institutional trust for Banks, Bigtechs, and Fintechs;

H4) The level of person trust is correlated with the level of system trust.

3. Data and Methodology

3.1. Data Collection

The first concern in order to fulfil the previously established goals of this dissertation was to gather data. Therefore, a valid primary source method of data collection was needed. Van Esterik-Plasmeijer and Van Raaij (2017) tested a model of banking system trust as an antecedent of bank trust and loyalty in the Netherlands. For that purpose, the previously discussed six determinants of trust (elected for this dissertation) were included and the scores on each determinant were evaluated and correlated with Person, System, and Institutional Trust. In their survey, respondents rated their personal bank, and another bank they were familiar with. Both banks were self-selected, and similar questions regarding the six determinants of trust were asked in relation to both institutions.

Thus, although the objectives of the authors differ from the ones of this research, the information extracted from the survey used in their work matches the required information for this research. Furthermore, the reliability of the method used by Van Esterik-Plasmeijer and Van Raaij (2017) was duly evaluated by them, cited by dozens of other authors, and confirmed with positive results. Therefore, the parts of the survey related with Person, System, and Institutional Trust were adapted and used for the purpose of this dissertation. However, for the questions related with the determinants of trust a 7-point likert was used instead of a 5-point, to give the respondent a wider range for classification, and comparison, between institutions. The differentiation between the different institutions is much more important in this research than in Van Esterik-Plasmeijer and Van Raaij (2017).

Added to that, this research also needed to be able to collect and evaluate information related to privacy and security in a similar way. Accordingly, this work's questions regarding perceived privacy and security are extracted from the research of Chellapa (2008) who assessed the role of perceived privacy and security in consumer's trust in electronic commerce, what is related at some degree with what this dissertation aims to investigate in terms of privacy and security. As such, and since the questions on this author's survey are positively framed (highest classification for the highest perception of privacy and security, and not for the level of concern) it makes sense to adapt the questions of Chellapa (2008) survey to ours. As a result, the survey used in this research can be divided into three sections.

In the first section, there are 2 questions which intend to record levels of Person Trust, Financial System Trust, measured with 10-point scales, where 1 corresponds to "no trust at all" and 10 to "complete trust". The second section is repeated three times, one for each type institution (banks, Bigtechs, and Fintechs). First, respondents are asked to select one institution of their choice, and express their level of trust in the institution chosen in a 10-point scale, where 1 corresponds to "no trust at all" and 10 to "complete trust". The following inquiries can be divided in two sets: The first set is adapted from Van Esterik-Plasmeijer and Van Raaij (2017) and here respondents are asked the extent to which they agree with 21 statements, on 7-point Likert scale (from "Completely Disagree" to "Completely Agree"). It aims at assessing the respondents' perception regarding the dimensions of trust (Competence, Stability, Integrity, Client Orientation, Transparency, and Value Congruence) in banks, Bigtechs, and Fintechs as AIS providers. The second set is adapted from Chellapa (2008) survey and it enables the measurement of perceived privacy and perceived security by asking the extent to which respondents agree with 11 related statements, in an equal scale as in the previous set. Finally, in the third section of the questionnaire, respondents are required to provide basic demographic information: Gender, Age, Region, and Occupation. This is essential to verify the level of representativeness of the sample, as well as to check if there are any recurrent classifications within the same demographic group.

The survey was distributed during the month of August via Google Forms, with the objective of allowing for online dispersion. With a completion rate of 100%, there were 133 valid responses to the survey. The demographics distribution is presented in Table 1.

Table 1. Demographics, by total number, by percentage and by cumulative percentage.

	Frequency	Percentage	Cumulative
Gender			
Female	54	40,60%	40,60%
Male	79	59,40%	100,00%
Age			
18 - 23	43	32,33%	32,33%
24 - 29	67	50,38%	82,71%
30 - 35	5	3,76%	86,47%
36 - 49	6	4,51%	90,98%
50+	12	9,02%	100,00%
Region			
North	1	0,75%	0,75%
Center	9	6,77%	7,52%
Lisbon Metropolitan Area	121	90,98%	98,50%
South	2	1,50%	100,00%
Occupation			
Studying	42	31,58%	31,58%
Working	83	62,41%	93,98%
Unemployed	8	6,02%	100,00%
Education			
12th Grade	8	6,02%	6,02%
Bachelor's Degree	34	25,56%	31,58%
Post-Graduate Degree	17	12,78%	44,36%
Master's Degree	70	52,63%	96,99%
PhD, MD	4	3,01%	100,00%

The way the second section of the survey is constructed depends on the ability of several statements: three or four for the determinants of trust, six for perceived privacy, and five for perceived security. As such, for the sample to be reliable the answers for statements that correspond to the same concept should be aligned and have high intercorrelations. In order to test the reliability and ensure the internal consistency of those statements as measures for each determinant, and for each institution, the Cronbach's Alpha was computed (Table 2).

Table 2. Internal Consistency of measurements with final dataset using Cronbach's Alpha.

	Bank Trust	Bigtech Trust	Fintech Trust
Competence	0,80	0,79	0,84
Stability	0,77	0,70	0,88
Integrity	0,84	0,86	0,89
Client Orientation	0,72	0,81	0,83
Transparency	0,89	0,85	0,90
Value Congruence	0,88	0,74	0,80
Perceived Privacy	0,89	0,93	0,95
Perceived Security	0,92	0,95	0,94

There are different reports and opinions about the acceptable values of Cronbach's Alpha, which range from 0.70 to 0.95 (Bland and Altman, 1997). According to Nunnally's criterion values above 0.80 indicate high reliability, and is 0.70 is the minimum threshold for what is considered "acceptable". Since the values of Cronbach's Alpha ranged between 0.70 and 0.95, the measures reliability are deemed as satisfactory for our study.

3.2. Methodology

As stated before, the main objective of this dissertation to compare the scores of banks, Bigtechs, and Fintechs in Institutional Trust and in the different determinants of trust discussed in the literature review (which are joined by perceived privacy and perceived security). For such purpose, the software used was MS Excel.

The process to compare the levels of Institutional Trust was straightforward. The mean of the scores, attributed by the survey respondents, in relation to their trust in each type of institution served as the comparable value of Institutional Trust between banks, Bigtechs, and Fintechs.

Keeping in mind that the goal was not to compare scores of each individual statement in relation to institutional trust, but to compare the levels of each determinant of trust between banks, Bigtechs, and Fintechs, the statements were grouped according to the determinant and institution they were related to. Then, the mean of each group represented the performance of each determinant according to the respondents evaluation, and was assumed as the value used to differentiate scores. As such, it enabled the comparison between the perceived levels of Competence, Stability, Integrity, Client Orientation, Transparency, Value Congruence, Privacy, and Security of the different institutions.

Furthermore, for both these assessments, the standard deviation was calculated alongside the mean. The value given by the standard deviation allowed us to see in which determinants the respondent's scores are more aligned and in which they are more diverse, in other words, where respondents tend to agree or disagree more. The means were tested with pair sample t-tests, to check if the differences between means (and therefore, between institutions' scores on the determinants) were statistically significant.

Afterwards, the focus was directed to assess the hypothesis presented earlier. MS Excel Data Analysis Tool was used to perform linear regressions with two objectives: find if the two variables correlation is statistically significant; and find the value of the coefficient of correlation (R^2), which measures how strongly the two variables are related.

For H1 (The evaluation of the determinants of trust (competence, stability, integrity, customer orientation, transparency, and value congruence) are correlated with the level of institutional trust for banks, Bigtechs, and Fintechs), three sets of regressions were done, one for each type of institution. The regressions used as independent variable the scores on the statements related to one of the determinants of trust. Therefore, for each institution type, there were six regressions. As for the dependent variable, it was the score of institutional trust of banks, Bigtechs, and Fintechs (individually).

Likewise, the assessment of H2 (The evaluations on perceived privacy and security are correlated with level of institutional trust for banks, Bigtechs, and Fintechs) followed the same logic. Three pairs of regressions were done, one for each type of institution. One of the regressions used as independent variable the scores on the statements related to perceived privacy, and the other the scores related on the statements related to perceived security. As for the dependent variable, it was the score of institutional trust of banks, Bigtechs, and Fintechs (individually).

For H3 (The level of system trust is correlated with level of institutional trust for banks, Bigtechs, and Fintechs), only three regressions were done, one for each type of institution. The independent variable was always given by scores on system trust from the first section of the survey, and the scores of institutional trust for banks, Bigtechs, and Fintechs were individually used as the dependent variable, once again.

Lastly, for H4 (The level of person trust is correlated with the level of system trust), it was required only one regression where the scores of person trust were used as the independent variable, and the scores of system trust were used as the dependent variable. Both were extracted from the first section of the survey.

4. Results

4.1. Scores of Institutional trust and Determinants of Trust

For the purpose of this research, the significance is assessed at a 95% confidence level. The average scores of institutional trust in banks, Bigtechs, and Fintechs are presented at the bottom of Table 3, being 1 the lowest possible grade, and 10 the higher and the best. Bigtechs, with a score of 6.76, are the ones with the highest score amongst the three types of institution. However, only the difference between the scores of Bigtechs and Fintechs, the lowest average score of the three with 6.43, was statistically significant. As for banks, with an average grade of 6,58, are in the middle and the difference to the other average scores is small, not even statistically significant to neither Bigtechs or Fintechs.

Table 3. Average Scores ofInstitutional Trust and of the Determinants of Trust for banks, Bigtechs, and Fintechs.

Determinants of Trust	**Banks**		**Bigtechs**		**Fintechs**	
(0-7 scale)	Mean	St.Dev	Mean	St.Dev	Mean	St.Dev
Competence***	5,35	0,97	6,11	1,06	5,67	1,15
Stability***	5,42	1,34	6,29	1,11	5,05	1,34
Integrity	5,40	1,29	5,27	1,40	5,31	1,23
Client Orientation	4,81	1,42	4,92	1,50	4,96	1,33
Transparency**	5,13	1,29	5,15	1,50	5,36	1,26
Value Congruence***	5,06	1,34	5,29	1,56	4,67	1,57
Perceived Privacy***	4,57	1,59	3,90	1,82	4,41	1,52
Perceived Security***	5,12	1,34	4,15	1,72	4,58	1,48
Institutional Trust* (0-10 scale)	6,58		6,76		6,43	

"***" - Difference between means of different institutions is statistically significant / "**" - Difference between means of different institutions is statistically significant, except between banks and Bigtechs / "*" – Difference is statistically significant only between Bigtechs and Fintechs

When looking at the mean scores for the determinants of trust (with perceived privacy and perceived security included) are also presented in Table 3. The average scores of the several determinants range from 4.57 to 5.42 for banks, from 3.90 to 6.29 for Bigtechs, and from 4.41 to 5.67 for Fintechs, where 1 is the lowest possible value and 7 is the highest and the best grade. The results show that the three types of institution have different score hierarchies for the eight determinants assessed.

For banks, the highest average scores, in descending order, are given to Stability (5.42), Integrity (5.40), and Competence (5.35). Those are followed by Transparency (5.13), Perceived Security (5.12), and Value Congruence (5.06). The lower average ratings are attributed to Client Orientation (4.81) and Perceived Privacy (4.57). The lowest standard deviation recorded is related to Competence (0.97), and the highest to Perceived Privacy (1.59).

As for Bigtechs, the highest average scores, in descending order, are associated with Stability (6.29) and Competence (6.11). Those are followed by Value Congruence (5.29), Integrity (5.27) and Transparency (5.15). The lower average ratings are given to Client Orientation (4.92), Perceived Security (4.15) and Perceived Privacy (3.90). As a matter of fact, the highest standard deviations are associated with these last two: Perceived Privacy (1.82), and Perceived Security (1.72). The lower standard deviations are related to Competence (1.06) and Stability (1.11).

Finally, in descending order, the highest average scores for Fintechs are attributed to Competence (5.67), Transparency (5.36), and Integrity (5.31). Those are followed by Stability (5.05) and Client Orientation (4.96). The lower average ratings are given to Value Congruence (4.67), Perceived Security (4.58), and Perceived Privacy (4.41). Once more, the lowest standard deviation is associated to Competence (1.05), and the highest is related to Value Congruence (1.57).

Competence is always one of the highest rated determinants for every type of institution. The differences between the institution's average scores on Competence are always statistically significant, according to the pair sample t-tests. Bigtechs are the ones perceived as more competent by the respondents (6.11), followed by Fintechs (5.67). Banks are the ones deemed as the less competent of the three (5.35). This determinant also records the lowest values of standard deviation in all types of institution.

Stability is the determinant with the highest average score in both Bigtechs (6.29) and banks (5.42). The differences between the institution's average scores on Stability are always found to be statistically significant, by the pair sample t-tests. The value for Bigtechs is the highest value recorded for any determinant, and also has one of the lower standard deviations. Fintechs are considered the less stable (5.05) by to our sample.

For Integrity and Client Orientation, none of the differences between the average ratings of the three institutions are statistically significant. Therefore, a comparative analysis is not relevant.

Regarding Transparency, the average score for banks (5.13) and Bigtechs (5.15) are very close. As such the difference between them is not statistically significant. By their turn, Fintechs have the higher average score on this determinant (5.36).

As for Value Congruence, the differences between the average scores for banks, Bigtechs, and Fintechs, are all statistically significant. Bigtechs (5.29) are the best performer on this determinant, followed by banks (5.06). Fintechs record the lower average score on this determinant (4.67).

Perceived Privacy is the determinant which records the lowest average score in the table, for Bigtechs (3.90). Furthermore, it is also the lowest average score of any determinant for Fintechs (4.41), and for banks (4.57). The differences between the means of the three types of institutions are all statistically significant.

Lastly, Perceived Security is also amongst the determinants with the lowest average score for Bigtechs (4.15) and Fintechs (4.58). As for banks, the score is relatively higher (5.12), and this determinant is not amongst the lower average ratings. All the differences between average scores are statistically significant.

4.2. Correlations of Person Trust, System Trust, Institutional Trust, and Determinants

As explained earlier, the coefficients of correlation are the measure that allow us to assess our hypothesis. It is used to measure how strongly two variables are related to each other. In Table 4, the coefficients of correlation (R^2) regarding the effect of Person Trust on System Trust, as well as the effect of System Trust on Bank Trust, Bigtech Trust, and Fintech Trust are presented. Additionally, in Table 4, the coefficients of the independent variables (X) are also presented, it is important to refer that in the results they are all positive, which implies positive relationships with the dependent variables. All the correlations are statistically significant, with the exception of System Trust and Fintech Trust. Person Trust has a significant correlation with System Trust, which matches the findings of Van Esterik-Plasmeijer and Van Raaij (2017). As for System

Trust, the stronger significant correlation is with Bank Trust (0.56), followed by Bigtech Trust (0.29).

Table 4. Coefficients of Correlation and Independent Variables Coefficients for Person Trust on System Trust, and System Trust on Bank, Bigtech, and Fintech Trust

Independent Variables	System Trust		Bank Trust		Bigtech Trust		Fintech Trust	
	R^2	X	R^2	X	R^2	X	R^2	X
Person trust	0,24	0,26	-	-	-	-	-	-
System Trust	-	-	0,56	0,63	0,29	0,34	0,16*	0,19

"*" - Not statistically significant correlation / "R^2" – Correlation Coefficient / "X"- Coefficient of the independent variable

In Table 5, the correlation coefficients (R^2) relative to the relationship between the determinants of trust and institutional trust, as well as the coefficients for the independent variables (X) are presented. All independent variables are statistically significant, except for the correlations between Competence and Bank Trust, and Perceived Privacy and Bank Trust.

Table 5. Coefficients of Correlation and Independent Variables Coefficients for the Determinants of Trust on Bank, Bigtech, and Fintech Trust

Independent Variables	Bank Trust		Bigtech Trust		Fintech Trust	
	R^2	X	R^2	X	R^2	X
Competence	0,19*	0,05	0,58	0,27	0,58	0,25
Stability	0,28	0,10	0,50	0,19	0,69	0,24
Integrity	0,33	0,13	0,65	0,23	0,75	0,30
Client Orientation	0,32	0,13	0,70	0,32	0,83	0,43
Transparency	0,33	0,11	0,56	0,18	0,76	0,40
Value Congruence	0,30	0,11	0,38	0,17	0,58	0,26
Perceived Privacy	0,28*	0,05	0,41	0,07	0,59	0,13
Perceived Security	0,40	0,10	0,36	0,07	0,54	0,15

*Not statistically significant correlation /"R^2" – Correlation Coefficient /
"X"- Coefficient of the independent variable

Although the further analysis of the coefficients of the independent variables is out of the scope of this dissertation, it is important to refer that in the results they are all positive, which implies

positive relationships with the dependent variables. Regarding Bank Trust, Perceived Security (0.40) is the determinant of trust with stronger correlation. The lowest correlation coefficient is related to Stability (0.28). The difference between the remaining correlation coefficients of the determinants of trust is very low and is ordered (in a descending manner) as follows: Transparency (0.33), Integrity (0.33), Client Orientation (0.32), and Value Congruence (0.30). As stated previously, both Competence (0.19) and Perceived Privacy (0.28) do not have statistically significant correlations with Bank Trust.

Concerning Bigtech Trust, all the independent variables are statistically significant. The determinant of trust with which the correlation is stronger is Client Orientation (0.70), followed closely by Integrity (0.65). On the other hand, the weaker correlations are with Perceived Security (0.36), Value Congruence (0.38), and Perceived Privacy (0.41). The other determinants' coefficients of correlation are ordered as follows: Competence (0.58), Transparency (0.56), and Stability (0.50).

Finally, for Fintech Trust, all the independent variables are statistically significant, as well. The determinants of trust with which the correlations are stronger are Client Orientation (0.83), Transparency (0.76), Integrity (0.75), and Stability (0.69). Although all the values are relatively high, the weakest correlation is with Perceived Security (0.54). The other determinants' coefficients of correlation are similar to each other and ordered as follows: Perceived Privacy (0.59), Value Congruence (0.58), and Competence (0.58).

5. Conclusions

Primarily, this study intends to compare the levels of Institutional Trust, and its determinants, across the three types of institution (Banks, Bigtechs, and Fintechs) as AIS providers, in Portugal. Furthermore, and with the goal of completing such analysis, this work also aims at understanding the strength of the correlations between the determinants of trust and institutional trust, and between System Trust and Institutional Trust for each type of institution. Lastly, the relationship between Person Trust and System Trust is relevant due to the geographic focus of this dissertation. The results show that this study contributes to trust measurement studies, applied in the financial industry. Particularly in what concerns the new AIS brought by PSD2, these results can be helpful for related future marketing decisions by banks, Bigtechs, and Fintechs.

Although Bigtechs are perceived as the most trustworthy institution amongst the three, the scores on Institutional Trust do not differ much between each other. It is only possible to conclude that the level of Institutional Trust in Bigtechs is higher than in Fintechs, the institution perceived as less trustworthy overall.

Regarding the determinants of trust and their scores, it is possible to conclude that the results are aligned with H1 (The evaluation of the determinants of trust (competence, stability, integrity, customer orientation, transparency, and value congruence) are correlated with the level of institutional trust for banks, Bigtechs, and Fintechs), with one exception: Competence is not correlated with Bank Trust. As such, the perception customers have about the competence of a bank is not related with their trust in that bank. Likewise, the results support H2 (The evaluations on perceived privacy and security are correlated with level of institutional trust for banks, Bigtechs, and Fintechs), with the exception of Perceived Privacy and Bank Trust, which correlation is not significant. Therefore, it is also a relevant conclusion that the perception customers have on the privacy of their information, stored by the bank, is not related with their trust in that bank. Moreover, it is important to mention that all the determinants of trust have a positive relationship with the level of Institutional Trust for banks, Bigtechs, and Fintechs.

As to H3 (The level of system trust is correlated with level of institutional trust for banks, Bigtechs, and Fintechs), the results show that System Trust is positively correlated to Bank Trust and Bigtech Trust. However, it is not correlated with Fintech Trust. As such, similarly to

H1 and H2, this hypothesis is only partially confirmed. Furthermore, it is an important conclusion of this research that the correlation of Bank Trust with System Trust is stronger than with any of the determinants of trust, as well as Perceived Privacy and Security, which is opposite to what happens with Bigtech Trust and Fintech Trust. This leads to the conclusion that the trust individuals have on the financial system has more influence on their trust in banks than any perception related to the determinants of trust, privacy, and security. The contrary is true for Bigtechs and Fintechs.

In what concerns H4, the results indicate that it cannot be rejected. This means that the level of interpersonal trust influences the trust in the financial system. As Person Trust is different across cultures, due to their distinct traditions, formality protocols, and relationship trust requirements, it serves as a benchmark for other dimensions' levels of trust, which are also dependent on the social setting. It is higher than System Trust and Institutional Trust, as expected (Van Esterik-Plasmeijer and Van Raaij, 2017).

Besides being considered the most trustworthy overall, Bigtechs are perceived as the most competent and the most stable. Furthermore, they are also the institutions with which individuals identify the most, in relation to their values. However, the relationship between Value Congruence and Bigtech trust is weak when compared to the other determinants. Likewise, Bigtechs are perceived as the least reliable to respect privacy and secure information, but both Perceived Privacy and Perceived Security have the weaker correlations (alongside Value Congruence) with the overall level of trust in Bigtechs. Despite that, Bigtechs are the institutions in which consumers trust the most. This goes in favor of the argument that consumers are willing to trade-off their personal information in return for value and access to their services (Kapko, 2012). The primary added values of mobile technologies are its speed and on-the-go quality, which is incompatible with adding requirements to increase privacy and security (Fife and Orjuela, 2012). However, the fact that neither Bigtechs nor Fintechs outperform banks significantly in Client Orientation is alarming, since these institutions argue that their user-centric focus is one of their main added values to customers relative to banks.

By their turn, banks are perceived as the most secure to provide personal information, and the most trustworthy to keep the privacy of such information. Although Perceived Privacy is not correlated with the overall level of trust in banks, Perceived Security represents the stronger correlation of any determinant with Bank Trust. This reinforces the idea presented by bank

representatives in Roland Berger's report (2019) that despite the responsibility in the recent global financial crisis, banks are still perceived as safe and secure, especially when comparing with other financial services providers. On the other hand, banks are deemed by as the less competent, yet there is evidence that their competence is unrelated with individual's trust in banks, as explained earlier. Additionally, they are also the institutions with the highest consideration for Integrity, which is interesting due to relevant number of bankruptcies and criminal prosecutions involving bank executives in Portugal, in the recent past, and the lowest for Client Orientation. Nonetheless, the scores on both are not significantly different across the institutions.

Lastly, Fintechs are considered to be more transparent in relation to their procedures and policies than banks or Bigtechs. However, these institutions are also perceived as the least stable, which is normal due to their nature: smaller enterprises that focus on a specific financial service. It is also possible to conclude that the determinants of trust correlation with Fintech Trust is stronger than both Bank Trust and Bigtech Trust. This means that a potential shift in individuals perception regarding any of these determinants would have a greater impact if it was related to Fintechs, than if it happened in any of the other institutions.

Overall, there is no apparent sign that banks are about to be overthrown as AIS market leaders due to the levels of trust in financial services providers. However, individuals seem to associate banks with the financial system, even more than with banks' own capabilities and attributes. Therefore, banks are much more subjectable to the political environment and what appears on the media channels than the other financial service providers, which puts them in a dangerous position. Since Bigtechs are already significantly outperforming in several determinants of trust and in the overall level of trust, although not significantly. As such, Bigtechs represent the major threat to banks in the Portuguese AIS market, at this moment. If these institutions strengthen their presence in the financial market post-PSD2, and keep gaining recognition as trustworthy financial services providers, banks' current position can be at their reach. By their turn, Fintechs can also aim to be important players in the AIS market, in the future. Despite being deemed as the least trustworthy in general, these institutions image disconnection with the financial system can be an important advantage in the near future. Intrinsically, Fintechs have more potential and independence to improve their image than the other players. By focusing customer policy on the determinants of trust (Van Esterik-Plasmeijer and Van Raaij, 2017) Fintechs can increase the levels of trust much more effectively than their competitors.

6. Limitations and Further Investigation

This dissertation main limitations concern the demographics of the sample. It was clearly not statistically representative of the Portuguese population: a large majority of the surveyed were from Lisbon Metropolitan Area, which tend to be more tech-savvy and open-minded. The lack of respondents from more provincial regions, where the mindset tends to be more conservative, can have influenced the results. Likewise, the evident predominance of younger demographic segments, of individuals aged between 18 and 29 years old, and the underrepresented of individuals between 30 and 49 years old in the final dataset, and as a key group of potential users of the AIS, it would have been better to increase their presence in the sample.

Furthermore, trust can also be related to characteristics of the individual that are not captured in this research data sample. Hansen (2012) found that financial knowledge, financial healthiness, and satisfaction also contribute to Institutional Trust.

Thus, further research on this topic could be done by studying study other drivers of consumer choice regarding financial services, if possible directly related to AIS, within a broader and more inclusive sample of the Portuguese population. Likewise, cluster analysis using the respondent's demographic data to find patterns that relate certain characteristics of respondents to their perceptions would also be relevant.

Finally, since the AIS market has only recently appeared, in the future it would be interesting to assess the evolution of the presence of banks, Bigtechs, and Fintechs in this market.

7. Appendix

A. Survey

A.1. Introduction

Assessment of Perceived Trust in Banks, Bigtechs, and Fintechs

Thank you for agreeing to participate in this survey!

This survey is a part of my dissertation to complete the MSc in Finance at Católica Lisbon School of Business and Economics. The dissertation aims to evaluate the consumer's trust in Portugal, in the three types of institutions (Banks, Bigtechs, and Fintechs) that are recently enabled by a revision of European Union's regulation to act as Account Information Service (AIS) providers.

In the revised directive, the European Union defines Account Information Services as “an online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider”. Simply put, they gather the information on the user’s various bank accounts and consolidate all of it in a single place, following the new and improved security and safety requirements of the European Union. Their purpose is to enable the user to have an overall view of its financial situation instantly, at any given moment.

The objective of this survey is to access your perception, regarding several specific dimensions of Trust, over the institutions that can offer Account Information Services (AIS) in Portugal: Banks, Bigtechs, and Fintechs.

In the first section, the intent is to evaluate the respondent's general level of trust in other people and in the financial system.

In the second part, the respondent will be asked to choose three institutions with which he is familiar with (one Bank, one Bigtech, and one Fintech) and answer the questions related to its institutional trust.

Lastly, the third part requires you to give out basic demographic information.

A.2. Personal and Systematic Trust

	No trust at all									Complete trust
	1	2	3	4	5	6	7	8	9	10
To what extent do you trust people in general? Please give a grade.										
If you had to express your trust in Financial System with a grade, what grade would you give?										

A.3. BANKS

Select a BANK (not necessarily one from the image above) with which you are familiar with. Preferably one that you are/were a client of, or if not, one with which you have a relatively informed perception of its service and practices.

BPI
Millenium BCP
Montepio
Santander
Novo Banco
BBVA
Bankinter
BiG
Caixa Geral de Depósitos
EuroBic
Banco CTT
OTHER

	No trust at all									Complete trust
	1	2	3	4	5	6	7	8	9	10
If you had to express your trust in this BANK at this moment, what grade would you give?										

A.4. BIGTECHS

Select a BIGTECH (not necessarily one from the image above) with which you are familiar with. Preferably one that you are/were a client of, or if not, one with which you have a relatively informed perception of its service and practices.

Amazon
Apple
Google
Facebook
Microsoft
OTHER

	No trust at all									Complete trust
	1	2	3	4	5	6	7	8	9	10
If you had to express your trust in this BIGTECH at this moment, what grade would you give?										

.

A.5. FINTECHS

"Organizations that have as a sole focus use technology to deliver digital financial products and services. These companies tend to be younger and aim to provide a more specific financial service rather than a portfolio of different products."

Select a BIGTECH (not necessarily one from the image above) with which you are familiar with. Preferably one that you are/were a client of, or if not, one with which you have a relatively informed perception of its service and practices.

Revolut
N26
Seedrs
Raize
ComparaJá.pt
doutorfinanças
OTHER

	No trust at all									Complete trust
	1	2	3	4	5	6	7	8	9	10
If you had to express your trust in this FINTECH at this moment, what grade would you give?										

A.6. Common Section – Institutional Trust

(Repeated three times, once for Banks, once for Bigtechs, and once for Fintechs).

Please answer the following questions based on the institution you previously chose.

To what extent do you agree with the following statements.

Statements	Completely Disagree 1	2	3	4	5	6	Completely Agree 7	Determinant of Trust
Knows exactly what is happening in the market.								COMPETENCE
Knows its clients and their financial needs.								COMPETENCE
Selects the right products for clients.								COMPETENCE
Is competent.								COMPETENCE
Is there for clients when they need.								STABILITY
Will not go bankrupt								STABILITY
Is financially solid.								STABILITY
Is large and strong.								STABILITY
Does not stay away when clients have problems.								INTEGRITY
Treats clients fairly.								INTEGRITY
Obeys the law and regulations.								INTEGRITY
Has integrity.								INTEGRITY
Responds quickly to questions asked by clients.								CLIENT ORIENTATION
Warns clients for wrong decisions.								CLIENT ORIENTATION
Puts the interest of the customer first.								CLIENT ORIENTATION
Is open about costs and risks of products and services.								TRANSPARENCY
Is open about procedures.								TRANSPARENCY
Communicates clearly.								TRANSPARENCY
Is transparent.								TRANSPARENCY
Is involved with society.								VALUE CONGRUENCE
Is involved in local activities.								VALUE CONGRUENCE
Contributes to a sustainable society.								VALUE CONGRUENCE

Statements	Completely Disagree 1	2	3	4	5	6	Completely Agree 7	Determinant of Trust
I am confident that I know all the parties who collect the information I provide.								PRIVACY
I am aware of the exact nature of information that will be collected.								PRIVACY
I believe I have control over how the information I provide will be used.								PRIVACY
I believe I can subsequently verify the information I provide.								PRIVACY
I believe my information will not be disclosed without my consent.								PRIVACY
I believe there is an effective mechanism to address any violation of the information I provide.								PRIVACY
I have confidence in the security of my transactions with this entity.								SECURITY
I am confident that the private information I provide will only reach this entity.								SECURITY
I do not believe inappropriate parties may deliberately view the information I provide.								SECURITY
I believe the information I provide will not be manipulated by inappropriate parties.								SECURITY
I do not believe that inappropriate parties may store the information I provide.								SECURITY

8. References

Afandi, E., & Habibov, N. 2013. “Pre-crisis and post-crisis trust in banks: Lessons from transitional countries”. Munich, Germany: Munich Personal RePEc Archive.

Arner, D. W., Barberis, J. & Buckley, R. P. 2016. “The evolution of fintech: a new post- crisis paradigm?”. Georgetown Journal of international Law, Vol. 47, No.4, pp. 1271-1319.

Bansal, Gaurav. 2017. “Distinguishing between Privacy and Security Concerns: An Empirical Examination and Scale Validation”. Journal of Computer Information Systems, Vol. 57, No.4, pp. 330-343

Barber, B. 1983. “The logic and limits of trust”. New Brunswick, NJ: Rutgers University Press.

BCG (2018). “Digital’s impact in the Portuguese Economy”.

Berry, Leonard L. 1995. "Relationship Marketing of ServicesGrowing Interest, Emerging Perspectives". Journal of the Academy of Marketing Science, Vol. 23, pp. 236-45.

Bland, J.M., & Altman, D.G. 1997. “Cronbach’s alpha”. BMJ, pp. 314-572

Chellappa, R.K. 2008. “Consumers’ trust in electronic commerce transactions: the role of perceived privacy and perceived security”.

Colangelo, G., Maggiolino, M. 2019. “From fragile to smart consumers: Shifting paradigm for the digital era”. Computer law & security review, Vol 35, No.2, pp. 173-181

Cortet, M. Rijks,T., & Nijland, S. 2016. “PSD2: The digital transformation accelerator for banks.” Journal of Payments Strategy & Systems, Vol. 10, No.1, pp. 13– 27.

Döderlein, Daniel. 2018. “What is the optimal mix between banks and FinTechs in the payments architecture?”. Journal of Payments Strategy & Systems Vol.12, No.2, pp. 122- 129.

Donnelly, Mary. 2016. “Payments in the digital market: Evaluating the contribution of Payment Services Directive II”. Computer Law & Security Review, Vol 32, pp 827-839

Dotti Sani, G.M., & Magistro, B. 2016. “Increasingly unequal? The economic crisis, social inequalities and trust in the European Parliament in 20 European countries”. European Journal of Political Research, Vol. 55, No.2, pp. 246–264.

Ennew, C., & Sekhon, H. 2007. “Measuring trust in financial services: the trust index”, Consumer Policy Review, Vol. 17, No.2, pp. 62-68.

European Banking Authority (2014). “Guidelines on the security of internet payments”

European Central Bank (2009). “Annual Report”.

European Central Bank (2018). “The revised Payment Services Directive (PSD2) and the transition to stronger payments security”.

European Central Bank (1999). Press release (September 23, 1999): “Monetary Policies Decisions”.

European Commission (2012). “Green Paper”.

European Commission (2007a). Press Release (December 12, 2007) :“Payment Services Directive: Commission encourages swift and coherent implementation at national level”.

European Commission (2007b). “Payment Services Directive: Frequently Asked Questions”.

European Commission (2018a). “Payment Services Directive: Frequently Asked Questions”.

European Commission (2018b). “Payment services: Consumers to benefit from cheaper, safer and more innovative electronic payments.”

European Payments Council (2004).“EPC Roadmap 2004-2010”.

European Payments Council (2017). “How can Application Programming Interface standardization be achieved in the context of the revised Payment Services Directive?”

European Payments Council (2017). “Payment threats and fraud trends report”.

EY (2019). Payments Newsletter, Vol.22.

Fife, E., & Orjuela, J. 2012. “The privacy calculus: Mobile apps and user perceptions of privacy and security”. International Journal of Engineering Business Management, Vol. 5, No.6, p. 7.

Friedman, B., Kahn, P.H., & Howe, D.C. 2000. “Trust Online”. Communications of the ACM, Vol. 43, pp. 34-40.

Fukuyama, Francis. 1995. “Trust: The social virtues and the creation of prosperity”. New York: Free Press.

Fungáčová, Z., Hasan, I., & Weill, L. 2019.“Trust in banks”. Journal of Economic Behavior & Organization, Vol. 157, pp. 452-476

Gambetta, Diego. 1988. “Can we trust trust?” D. Gambetta, ed. Trust: Making and Breaking Cooperative Relations. Blackwell, New York.

Ganesan, Shankar. 1994. “Determinants of Long-Term Orientation in Buyer–Seller Relationships”. Journal of Marketing, Vol. 58, pp. 1–19.

Garbarino, E., and Johnson, M.S. 1999. “The different roles of satisfaction, trust, and commitment in customer relationships”. Journal of Marketing, Vol. 63, No.2, pp. 70–87.

Grayson, K., Johnson, D. & Chen, D.F. 2008. “Is Firm Trust Essential in a Trusted Environment? How Trust in the Business Context Influences Customers”. Journal of Marketing Research, Vol. 45, pp. 241–57.

Hansen, Torben. 2012.”Understanding Trust in Financial Services: The Influence of Financial Healthiness, Knowledge, and Satisfaction”. Journal of Service Research, Vol. 15 (3), pp. 280-295.

Hartmann, Maren. 2011. Mobile privacy: Contexts. In S. Trepte & L. Reinecke (Eds.), “Privacy online: Perspectives on privacy and self-disclosure in the social web”, pp. 191–204. New York: Springer.

Hatfield, Jacqui. 2017. “Innovation in payments and the revised Payments Services Directive”. Journal of Payments Strategy & Systems, Vol 11, 78-80.

Hoffman, D.L., Novak, T.P. 1996. “Marketing in hyper media computer-mediated environments: Conceptual foundations”. Journal of Marketing, Vol. 60, No.3, pp. 50-117.

Hurley, R., Gong, X., & Waqar, A. 2014. “Understanding the loss of trust in large banks”. International Journal Of Bank Marketing, Vol. 32, No.5, pp. 348-366.

Janczuk, Agnieszka. 2010. ,”Legislative Development: The Single Payments Area in Europe”, Columbia Journal of European Law, Vol. 16, pp. 321-335.

Jin, J.. & Ahn, G.J. 2006. “Role-based access management for ad-hoc collaborative sharing”. in Proc. 11th SACMAT, pp. 200–209.

Kantsperger, R., & Kunz, W.H. 2010. “Consumer trust in service companies: a multiple mediating analysis”. Managing Service Quality, Vol. 20, No.1, pp. 4-25.

Kaplan, A. M., & Haenlein, M. 2010. “Users of the world, unite! The challenges and opportunities of social media”. Business Horizon, Vol. 53, No.1, pp. 59–68.

Keen, Peter G.W. 2000. “Ensuring e-trust’’. Computerworld, Vol. 34, p. 46.

KPMG (2011). “Privacy Security Issues Hamper Wider Growth of Mobile Banking, Despite Increasing Consumer Acceptance”.

Krumay, B., & Oetzel, M.C. 2011. “Security an privacy in companies: State-of-the-art and qualitative analysis”. In Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security, pp. 313–320.

Landau, Susan. 2008. “Privacy and security: a multidimensional problem”. Communications of the ACM, Vol. 51, No.11, pp. 25-26.

Lewis, J., & Weigert, A. 1985. “Trust as a social reality”. Social Forces, Vol. 63, pp. 967-985

Mavromati, Despina. 2008. “The Law of Payment Services in the EU: The EC Directive on Payment Services in the Internal Market”, Kluwer Law International, pp. 189–228.

Mayer, R. C., Davis, J.H., & Schoorman, F.D. 1995. "An integrative model of organizational trust". Academy of Management Review, Vol. 20, pp. 709-734.

McKnight, D. H., Choudhury, V., and Kacmar, C. 2002. “Developing and Validating Trust Measures for E-Commerce: An Integrative Typology”. Information Systems Research, Vol.13, No.3, pp. 334-359.

Meuter, M.L., Ostrom, A.L., Roundtree, R.I., & Bitner, M.J. 2000. “Self-Service Technologies: Understanding Consumer Satisfaction With Technology-Based Service Encounters”. Journal of Marketing, Vol. 64, No.3, pp. 50-64.

Miyazaki, A., & Krishnamurthy, S. 2002. "Internet Seals of Approval: Effects on Online Privacy Policies and Consumer Perceptions". Journal of Consumer Affairs, Vol.36, No.1, pp. 28-49

Moorman, C., Deshpande, R., & Zaltman, G. 1993. "Factors Affecting Trust in Market Relationships". Journal of Marketing, Vol. 57, pp. 81-101.

Morgan, R. M., & Hunt, S.D. 1994. “The Commitment-Trust Theory of Relationship Marketing”. Journal of Marketing, Vol. 58, pp. 20–38.

Pirson, M. and Malhotra, D. 2008. ‘‘Unconventional insights for managing stakeholder trust’’. MIT Sloan Management Review, Vol. 49, No.4, pp. 43-50.

PwC (2016). “Central Banking 2020: Ahead of the curve”.

Roland Berger (2019). “Adapt or die? Why PSD2 has so far failed to unlock the potential of Open Banking”.

Rotter, Julian B. 1967. “A new scale for the measurement of interpersonal trust”. Journal of Personalily, Vol. 35, pp. 651-665.

Scheja, O., & Machielse, W. 2019. “The NextGenPSD2 Framework in a Pan-European PSD2 Account Access Context”. Journal of Payments Strategy & Systems, Vol. 13, No. 1, pp. 54-65.

Schneiderman, H., & Kanade, T. 2000. “A statistical method for 3D object detection applied to faces and cars”. International Conference on Computer Vision.

Schueffel, Patrick. 2016. "Taming the Beast: A Scientific Definition of Fintech." Journal of Innovation Management, Vol. 4, No.4, pp. 32-54.

Sekhon, H., Ennew, C., Kharouf, H., & Devlin, J. 2014. “Trustworthiness and trust: Influences and implications”. Journal of Marketing Management, Vol. 30, pp. 409–430.

SEPA (2008a). “Credit Transfer Rulebook”

SEPA (2008b). “Cards Framework”.

SEPA (2009). “Direct Debit Rulebook”

Shapiro, Susan P. 1987. “The social control of impersonal trust”. American Journal of Sociology, Vol.93, pp. 623-658.

Sheppard, B.H., and Sherman, D.M. 1998. “The grammers of trust: A model and general implications”. Academy of Management Review, Vol. 23 (3), pp. 422–437.

Sirdeshmukh, D., Singh, J., & Sabol, B. 2002. “Consumer Trust, Value, and Loyalty in Relational Exchanges”. Journal of Marketing, Vol. 66, pp. 15-37.

Stewart, K.A., & Segars, A.H. 2002. "An Empirical Examina tion of the Concern for Information Privacy Instrument". Information Systems Research, Vol.13 (1), pp. 36-49.

Van Esterik-Plasmeijer, P.W., & Van Raaij, W.F. 2017. “Banking system trust, bank trust, and bank loyalty”. International Journal of Bank Marketing, Vol. 35, No.1, pp. 97–111.

Van Raaij, W.Fred. 2009. “How does the financial sector regain confidence?”. Me Judice, Vol. 2.

Wandhöfer, Ruth. 2009. The Payment Services Directive: Why the European payments industry needs to prepare for significant implementation challenges Journal oents Strategy & Systems, Vol. 2, No. 4 , pp. 400-409.

Warren, S., & Brandeis, L. 1890. “The Right to Privacy”. Harvard Law Review, Vol. 4 (5), pp. 193–200.

Westin, A. F. 1967. “Privacy and Freedom”. Athenaum, New York.

Ying, X., & Wu, X. 2011. “On link privacy in randomizing social networks,” Knowledge and Information Systems, Vol. 28, No.3, pp. 645-663.