FinTech: The role of Perceived cybersecurity and Organizational trust

Investigating from a customer perspective technological acceptance in Sweden.

David Laurent, Robin Sinz

Department of Business Administration
Master's Program in Finance
Master's Thesis in Business Administration III, 30 Credits, Term 2019
Supervisor: Jörgen Hellström
Acknowledgements

We would like to express gratitude to our supervisor Jörgen Hellström for his unlimited effort in supporting and helping us during the thesis writing process. We would like to thank him for his valuable insights and guidance as well as his feedbacks regarding the current topic.

We are also thankful for the support from Umeå University’s administration for guiding and helping us with the collection of the student email addresses. We would like also to extend our appreciation to all students who participated in the survey without which we could not have reached our aim.

David Laurent
Contact: david.laurent@mail.novancia.fr

Robin Sinz
Contact: robin_sinz@web.de
Abstract:

Context: The advent of the Information and Communication Technologies mostly referred to “digitalization”; offers a new paradigm. Information technology is now perceived as a disruptive innovation capable of shaking up the traditional financial industry. On one side and as a result of the former trend, a new taxonomy emerged under the name of “FinTech” corresponding to the embracement of “digitalization”. FinTech is implicated in the process of disintermediation through innovation. On the other hand and due to the recent incidents at the macroeconomic level such as the 2008 financial crisis or even more recently the Snowden case; the regulatory environment is undergoing drastic changes. Even though the changing regulatory environment firstly acted as a catalyst by promoting the FinTech phenomenon into the spotlight, it inherently touched upon one of the prominent challenges of “FinTech”: to the extent Information Security. Along the line, the FinTech ecosystem which is symbolized by the “Always Available” expression conveys an explicit statement which is yet challenged by the threat of cyberattacks and emphasized by the duality between availability and security. The existing paradox reasserts the growing need for trust from a customer perspective.

Purpose: In this thesis, the authors aimed to investigate the information security and consumer trust challenges within the FinTech ecosystem by empirically testing the customer’s perceptions on the variables that are likely to affect technological adoption.

Design/Methodology/approach: A cross sectional quantitative study was conducted with the distribution of a self-completion questionnaire to FinTech customers in Sweden. The designed conceptual model was built on the previous work of Stewart & Jürjens (2018). Stewart and Jürjens (2018) extended the TAM model by considering: Data Security, Customer Trust, Value Added, User Design Interface and FinTech Promotion. In this thesis, the authors adapted Stewart and Jürjens model (2018) by redefining “Data Security” and “Customer Trust”. Three regressions have been performed: one binary logistic regression and two multiple regressions.

Findings: We first ran a principal component analysis in order to reduce dimensionality within our questionnaire. We performed a PCA with an oblique rotation which helped us to produce factor scores. Based on the binary logistic regression, we found out that only Perceived Usefulness and Device security was significantly affecting our respondent’s payment intention. The multiple regression intending to predict the respondent’s intention to use based the on the factor scores from the PCA, revealed that Perceived Usefulness, Usability & ergonomics, Device security and Organizational trust were significant. Lastly, the final regression suggested that Overall trust and security were significantly affecting the respondent’s intention to use. In essence, it appeared that both dimensions are affecting the technological acceptance of users of mobile payment applications.

Research Limitations/implications: There are multiple limitations to our study, the first one being the use of a convenience sampling. Therefore, our results lack of generalizations. Yet, the results of our study confirm what the antecedents of customer’s intention to use mobile payment applications are, to the extent that both security and trust matter.
Table of contents

1. Introduction ........................................................................................................................................ 1
   1.1 Background .................................................................................................................................. 1
   1.2 Problem Discussion ....................................................................................................................... 2
      1.2.1 Evolution of the finance industry: e-finance, Digital Finance and FinTech ..................... 2
      1.2.2 FinTech ecosystem and challenges ....................................................................................... 3
      1.2.3 Regulatory framework: The importance of information security and Trust .............. 3
   1.3 Problem Formulation ..................................................................................................................... 6
   1.4 Purpose ......................................................................................................................................... 7
   1.5 Definitions of terms ....................................................................................................................... 8

2. Background and delineations ............................................................................................................... 9
   2.1 The FinTech’s ecosystem: dynamics and challenges ................................................................. 9
   2.2 The Regulatory framework ........................................................................................................ 11
   2.3 Information security challenge ................................................................................................... 12
      2.3.1 Context .................................................................................................................................. 12
      2.3.2 FinTech and Information Security ........................................................................................ 13
      2.3.3 Cybersecurity and Information Security: commonality and delineation ..................... 15
      2.3.4 Cybersecurity within FinTech ............................................................................................... 16
   2.4 Trust and traditional finance ........................................................................................................ 17
      2.4.1 Trust conceptualizations ......................................................................................................... 18
         a Personality theory ...................................................................................................................... 18
         b Risk expectations theory .......................................................................................................... 18
         c Institutional theory ................................................................................................................... 19
      2.4.2 Institutional trust and bank crisis .......................................................................................... 20
      2.4.3 FinTech: Offline and Online trust ........................................................................................ 21

3. Theoretical background and Literature review .................................................................................. 23
   3.1 Theory of Reasoned Action (TRA) ............................................................................................... 23
   3.2 Technological Acceptance Model (TAM) .................................................................................... 24
   3.3 Extended Post Acceptance Model (EPAM) .................................................................................. 24
   3.4 Unified Theory of Acceptance and Use of Technology (UTAUT) .......................................... 25
   3.5 Conceptual model and argumentation ......................................................................................... 25

4. Methodology ...................................................................................................................................... 31
   4.1 Choice of subject .......................................................................................................................... 31
   4.2 Research approach ....................................................................................................................... 31
   4.3 Fundamental assumption ............................................................................................................. 31
8.2.2 Managerial contribution ................................................................. 74
8.2.3 Societal and ethical aspects................................................................. 74
8.2.4 Limitations......................................................................................... 75
8.3 Future Researches .................................................................................. 76
8.4 Truth criteria in social research................................................................. 76
  8.4.1 Reliability ......................................................................................... 76
  8.4.2 Replicability ....................................................................................... 77
  8.4.3 Validity ............................................................................................... 77

Appendix 1: Questionnaire ........................................................................... 85
Appendix 2: Descriptive statistics................................................................. 93
Appendix 3: Cronbach’s alpha ............................................................... 95
Appendix 4: Normality PP Plot and Histogram ........................................... 96
Appendix 5: Original multiple regression on the conceptual model .......... 97
Appendix 6: Multiple regression with overall security and trust as predictors 98

List of figures:

Figure 1. Major participants in the FinTech ecosystem .............................. 9
Figure 2. FinTech ecosystem ....................................................................... 10
Figure 3. Relationship between cybersecurity and other security domains .... 16
Figure 4. Conceptual model ........................................................................ 30
Figure 5. Process and expected outcome from the factor analysis ............ 38
Figure 6. Gender repartition ........................................................................ 42
Figure 7. Age repartition ............................................................................. 43
Figure 8. Faculty repartition ........................................................................ 43
Figure 9. Intention to use mobile payment applications ................................ 44
Figure 10. Ranking of mobile payment services by usage ......................... 45
Figure 11. Eigenvalues scree plot ................................................................. 49
Figure 12. Revised conceptual model .............................................................. 59

List of tables:

Table 1. Variables and their origins .............................................................. 35
Table 2. Factor analysis and variable coding ................................................. 47
Table 3. KMO and Barlett’s test .................................................................. 48
Table 4. Communalities ................................................................................. 49
Table 5. Total variance explained ................................................................. 50
Table 6. Pattern matrix .................................................................................. 51
Table 7. Reliability analysis ......................................................................... 52
Table 8. Factor scores and interpretations..............................................................53
Table 9. Robust binary logistic regression ...............................................................53
Table 10. Pearson correlation for our conceptual model ...........................................55
Table 11. Robust multiple regression on our conceptual model ...............................56
Table 12. Pearson correlation overall security and trust ..........................................57
Table 13. Robust multiple regression with overall security and trust ..........................58
Table 14. Comparison of the theoretical model and revised model based on PCA ........59
1. Introduction

1.1 Background

As Harari (2015) articulated in his best seller Homo Deus; Humanity portrayed at the dawn of the third Millennium is exposed to a peculiar situation, where its former woes are no longer perceived as unreachable challenges but rather as manageable ones. The Human Agenda has shifted and one of its main concerns now relies on the Information and Communication Technology (ICT). The last decade has been at the center of the discussions by addressing the diverse substantial changes within the finance and banking industry (Nicoletti, 2017, p. 4).

Such discussions were unquestioningly motivated by various triggering elements; for instance, the different financial/economic crisis, followed by the changing regulatory environment and finally the behavioral customer changes (Nicoletti, 2017, p. 4). The advent of Information and Communication Technology (ICT) has participated to the adoption and diffusion of what is referred to as “digitalization”.

In essence, digitalization simply characterizes a new technological trend which disrupted the order of things, by for instance expanding connectivity, speed and processing of information which led to improve the efficiency and delivery of traditional tasks (Gomber et al., 2017, p. 537). The impact of digitalization within the field of finance is commonly referred to digital finance, encompassing all electronic potential products/services that the financial sector could offer (Banks 2001; Gomber et al., 2017, p. 539). Along this line, the Digital Finance Institute (2015) had described digital finance in a different way by outlining the innovative aspect of startup companies seeking to both integrate and distribute digital banking, mobile solutions and delivery platforms.

Even though the former integration and distribution is not exclusively the role of startups, the companies delivering such innovative business models, are often characterized as “FinTech” corporations (Gomber et al., 2017, p. 538). One sure thing is that digital transitioning has been the major catalyst behind the “FinTech” phenomenon (Nicoletti, 2017, p. 4). “FinTech” corresponds to a neologism contracting the terms “Financial” and “Technology” and refers to an emerging taxonomy within the financial Industry (Gai et al., 2018, p. 262) considered to be the most disruptive element of digital finance (Gomber et al., p. 542). The rapid expansion of the FinTech industry relies on the combination of three key drivers which are the favorable regulatory environment, the current globalization as well as the technological disruption.

Nonetheless, this highly expanding industry has to carry on while considering peculiar challenges which may place its expectancy at risk. One of these challenges has been booming in the recent years due to the different media coverages relaying information and data leaking, outlining information security as a hot button, subject to both challenges and opportunities.
1.2 Problem Discussion

1.2.1 Evolution of the finance industry: e-finance, Digital Finance and FinTech

During the past decade, one neologism has benefited from the spotlight and even been characterized as the hot button; this word is “FinTech” (KPMG, 2018). A retrospective on the evolution of the finance industry is beneficial to fully comprehend the ins and outs of FinTech’s phenomenon. In this perspective, the review of three major trends “e-Finance” “Digital Finance” and “FinTech” in terms of terminological commonalities; may provide the cornerstone to comprehend, delineate and contextualize the FinTech’s phenomenon and its disputes.

In essence in the 2000’s, the term “e-Finance” characterized the use of information and communication technologies within the financial industry (Gomber et al., 2017, p. 541). The literature is often portrayed by a lack of agreement amongst scholars who have usually defined the key terms “finance” or “electronic” differently hence producing various understandings of what is “e-Finance” (Gomber et al., 2017, p. 541). To illustrate this statement let us consider the “electronic” dimension. The “electronic” dimension has often been depicted by a duality between either including in its definition all Information Communication Technology (ICT), or in opposition comprising the Internet Technology (Gomber et al., 2017, p. 541). In other words, the ongoing discussions addressed which technology should be included in the definition of the word “electronic”.

Nevertheless, considering a financial point of view, “e-Finance” is seen as the disintermediation and re-intermediation between the financial institutions and market (Petzel, 2005). Drawing out on this particular interpretation of “e-Finance” allows us to link “FinTech” to “e-Finance”. In fact, “FinTech” has been defined as the disruptive innovation which is disintermediating or re-intermediating the financial industry by proposing unique technologically based solutions (Gomber et al., 2017, pp. 538-541; Nicoletti, 2017, p. 1).

In conclusion, the literature regards “e-Finance” and “Digital Finance” as quasi synonyms (Gattenio, 2002, p. 49), yet the only delineation between the former three terminologies (i.e. e-Finance, Digital Finance, FinTech) is the context. In such manner, “e-Finance” is regularly used to refer to the early use of the Information Communication Technology (ICT) in the financial sector; while “Digital Finance” characterized the extensive digitalization within the same industry. Lastly “FinTech” emphasizes the innovation and technological advancement, since most FinTechs are not originating from the financial sector (Gomber et al., 2017, p. 542). The distinction between the financial trends put in perspective the essence of “FinTech”. Additionally, FinTech, according to KPMG (2018), gained momentum during the first half of year as the investments expanded.
1.2.2 FinTech ecosystem and challenges

FinTech appears to be at its core highly disruptive, and the innovative disruption as well as its development legitimizes both from a practical and academic point of view the need to investigate its ins and outs. As it has been previously mentioned, the neologism (i.e. FinTech) and its delineation underline two significant elements: the first highlighting its innovative/technological development and the second stressing out the consequences of the former onto the traditional financial industry. Extending on the latter element, Lee and Shin (2018, p. 35) postulated that the technological breakthrough allowed FinTechs to disintermediate and challenge the traditional financial institutions by emphasizing the importance for many players to either develop internal capabilities or invest in “FinTech” in order to remain competitive.

The complex and yet novel nature of the growing phenomenon demands a comprehensive understanding of its ecosystem to identify the different protagonists within the industry and pinpoint not only its dynamics but also its challenges. According to Lee & Shin (2018, p. 37) there are five elements or dimensions that need to be considered to grasp the FinTech ecosystem. The different players are all contributing in shaping the FinTech ecosystem which is categorized as simultaneously competitive and collaborative. The growing investments within the FinTech sector have led to breakthrough advancements in multiple fields such as peer to peer, customer intimacy, payments, personal financial management, and underbanked innovation (Freij, 2018, p. 35). Yet, the competitive environment and profound changes currently occurring provide thereby the touchpoints which are likely to represent challenges that both FinTechs and financial institutions would have to deal with (Lee & Shin, 2018, p. 43).

Lee & Shin (2018, p. 43) extended by introducing the challenges in six manners:

1) Investment management challenge.
2) Customer management challenge.
3) Regulation challenge.
4) Technology integration challenge.
5) Security and privacy challenge.
6) Risk management challenge.

1.2.3 Regulatory framework: The importance of information security and Trust.

On one hand, we argue that the regulatory framework has merely acted as a catalyst for the FinTech industry and as such, different events which occurred at the macroeconomic level enacted innovation in the financial industry. Substantially, the evolution of the financial industry is driven by the regulatory changes (Freij, 2018, p. 21). According to Freij (2018, p. 22), the ongoing changes and future regulatory changes within the finance sector, represent the ultimate issue as they require time, investment and management. Beside the regulatory aftermath created by the financial crisis in 2008, the crisis created another drawback. In fact, the weakening of the global financial system highly discredited the banking industry that was held responsible of the overexposure and use of mortgage backed derivatives while its incapacity to deal with credit risks and operational risks taken gave the final blow.
In conclusion some institutions went bankrupted and at the same time lost credibility and trust in the eyes of their customers (Knell & Stix, 2015, p. 995). One the other hand, the current state of affairs especially after the Snowden case in 2013 has brought a lot of attention to the information security topic. As a result of the different media coverage, information security has become one of the top priorities notably in the financial sector (Newman, 2016a; cited in Kryparos, 2018, p. 44). The turning point is 2016, where the recurrence and scale of these events took a step further.

Major scandals were exposed, compromising information sensitive for both customers and corporations (Kryparos, 2018, p. 44). To fully understand the span of the cyber criminality and its consequences, it is necessary to put it in perspective with numbers. According to Verizon Data Breach Investigations report (DBIR), the industry which has been reporting the most security data breaches in 2016 was the financial one, counting 471 breaches. The growing awareness and concern about information security stems from the fact that the threat of global cyber-attacks is real. Recent literature attempted to solve various FinTech problems where a number of recent investigations have outlined the importance of security and privacy development (Gai et al., 2018, p. 262).

According to Gai et al. (2018, p. 263), the data and privacy issue within the FinTech environment is characterized by three dimensions: namely business operations, outsourcing and financial privacy. Nevertheless, information security is subject to many controversies since its definition has been different and approached from a technical perspective (Safa et al., 2015). In contrast, and as mentioned by Mitnick and Simon (2002, p. 4), data security should not be solely categorized as either an item or asset, but rather perceived as a process. Considering data security as a process permits to broaden the focus by including the human perspective. Furthermore, Werlinger et al. (2009) mentioned that human dimension is noteworthy since it includes a crucial perspective which is the role of organization’s leaders and employees onto the data security topic.

The concerns have been shifting to place information security as its peak; yet the traditional solution to software vulnerability is heavily relying on “security through obscurity” strategy. The latter describes a strategy relying on isolation” and “limited access” considered to be no longer feasible and mostly delusional in a changing environment based on open network and web technologies (Kryparos, 2018, p. 47). These features fully embraced by the FinTechs reaffirm the existing tension between the solutions promoted and the challenges faced.

To the extent, FinTechs were able to develop customized solutions tapping into fundamental needs so far undermined by traditional financial institutions (Kryparos, 2018, p. 43). To illustrate this, the PWC’s Global FinTech report (2017) exposed two interesting insights. In the PWC report, one central theme has been the threat represented by the nontraditional financial services providers within the upcoming five years; where 80% of the incumbents perceived that their businesses will be at risk (PWC, 2017, p. 5). The second theme exposed was the growing demand or forecasted consumption of nontraditional financial service providers where the survey indicated that while the consumption is set to increase by 30 % only 39% of consumers were considering to solely using traditional service providers (PWC, 2017, p. 5).
Meanwhile, the implementations of the Payment Services Directive 2 (PSD2) and the General Data Protection Regulation (GDPR) have boosted the compliance and regulatory requirements by addressing the information security and implicitly the construct of trust. The topic of information security appears due to its nature to represent an inherent risk for FinTechs and should be part of their risk management strategy as future data breaches will now be financially penalized with a fine accounting up to 4% of the annual turnover or set to EUR 20 million whichever is higher (Kryparos, 2018, p. 48).

Consequently, the rapid expansion of the phenomenon and the challenges represented, reasserts the need for recent and up to date awareness on FinTech (Gai et al., 2017, p. 262). The problem which arouse by enabling the simplification of the customer experience, is that the entire attention has shifted to the customer side which eventually echoed for the FinTechs to ensure a viable solution to the “availability” and “security” paradigm.

One issue which has been exposed by Teigland et al. (2018) is that both trust and trust in the information security features is needed to assure that customers are joining the FinTech movement. Henceforth, how can FinTechs guarantee their customers which are essentially on the Internet of Things (IoT), a service highly available while also acknowledging that each potential user can also be a threat? The reality that is facing FinTechs induces a dilemma where they should be capable of trusting that the customer using its services is not impersonating someone else (Kryparos, 2018, p. 48). Subsequently the concept of trust appeared be intimately linked to security. Apart from the legal compliance, information security reasserts the increasing need for trust from both a customer and firm perspective (Kryparos, 2018, p. 47).

As we have formerly expressed, the complexity depicting the FinTech phenomenon results from the duality between two features that FinTechs are supposed to exhibit: namely “security” and “availability”. To the extent, the duality extends to portray the FinTech’s penultimate issue which is the need to build a trust mechanism while ensuring security. The complexity of the objective is perceived to be one of the reasons why consumers are reluctant to shift to the non-traditional financial service provider. Consequently, the presupposed interrelation between information security and trust in the context of FinTech could constitute the necessary elements promoting technological acceptance amongst consumers.

In this line of argument, technological acceptance depicts the ultimate challenge for FinTechs. There are multiple theories addressing the topic of technological acceptance within the literature. Even though not all the theories are using the terminology “technological acceptance”, most of them approach the topic by investigating the field of consumer behavior in relation to technologies such as Theory of Reasoned Action (TRA), Expectation Confirmation Theory (ECT), Extended Post Acceptance Model theory (EPAM) and Technological Acceptance Model theory (TAM). Bearing this in mind, Stewart & Jürjens (2018) are the only scholars who addressed the two notions of “Trust” and “Security” with a FinTech perspective, where they published an empirical study of the key factors influencing the technological adoption of FinTech in Germany.
The study further developed the Technology Acceptance model (TAM) by incorporating novel dimensions inspired by the Wang et al. (2003) model, which resulted in a model proposing five dimensions: Data Security, Customer Trust, Value Added, FinTech Promotion and User Design Interface. Stewart & Jürjens (2018, p. 122) concluded that Data Security (DS), Customer Trust (CT) and User Design Interface (UI) were relevant regarding the FinTech adoption.

We argue in the line of Stewart & Jürjens (2018, p. 113) who explicitly indicated the need to: “highlight the necessary perspectives for the FinTech adoption process”. In fact, in this thesis, we argue that peculiar incidents at the macroeconomic level whether in the form of financial crisis or cyber-criminality, have profoundly reshaped the regulatory environment. The inevitable changes occurring at a higher pace in terms of consistency and significance led to disrupt and create a favorable regulatory environment currently driving innovation within the financial industry. Innovation which is conveyed by FinTech’s and their ability to innovate through disintermediation; by proposing tailored technologically driven solutions responding to undermined consumer’s needs. The apparition of these nontraditional service providers puts at risk different actors within the FinTech’s ecosystem. However, the new perspective given by this “FinTech” phenomenon is confronted to a paradox. A dilemma which is stated as the existing tension between their promises to be “always be available” and at the same time “be secured”.

In this regard, due to the different incidents at the international scene and the risk of global cyberattacks, the topic of information security is relevant both from a practitioner perspective as well as academic one. Lastly, due to the modern cybersecurity issue and its impact onto the financial industry, we argue that the concept of trust needs to be addressed in order to potentially and simultaneously solve the information security and technological acceptance that FinTech faces. Creating trust through cybersecurity and security expertise will therefore represent the competitive edge needed in this highly aggressive environment and impact FinTech adoption.

### 1.3 Problem Formulation

As we have previously exposed, the ultimate challenge for FinTechs is to ensure technological acceptance. As such, in this thesis, we will be investigating technological acceptance by looking at customer’s intention to use mobile payment applications. Ultimately, we are seeking to empirically test customer’s perceptions on the antecedents causing their intention to use mobile payment applications.

In this regard we propose the following research question:

| What is the role of Perceived cybersecurity and Organizational trust on the customer’s intention to use mobile payment applications? |
1.4 Purpose

This thesis aims to investigate from a customer perspective, the technological acceptance of FinTech payment solutions by considering the role of Perceived cybersecurity and Organizational trust. We argue in the line of Stewart and Jürjens (2018) who proposed a revised version of the Technological Acceptance Model (TAM) by integrating the notion of “Data Security” and “Customer Trust”. Nevertheless, we share a different conceptualization of the notion of “Data Security” and “Customer Trust” thereby reviewing and adapting their research model by extending the notion of “Data Security” to “Perceived cybersecurity” and “Organizational trust” as stemming from the online trust literature (i.e. trust in the technology and trust in the organization). In order to achieve this aim, the authors will use a quantitative research design and more specifically hypotheses testing in order to verify the model designed with the selected variables amongst Swedish FinTech mobile payment customers.
1.5 Definitions of terms

**Digitalization**: new disruptive technological trend expanding connectivity, speed and processing of information thereby drastically improving the delivery of traditional tasks (Gomber et al., 2017, p. 537).

**Digital finance**: The literature regards “e-finance” and “digital finance” as quasi synonyms (Gattenio, 2002), the only difference is “digital finance” characterized the extensive digitalization in the financial industry.

**e-finance**: “e-finance” is seen as the disintermediation and re intermediation between the financial institutions and market (Petzel, 2005)

**FinTech**: the term originates from the contraction of the two terms Financial and Technology (Gai et al., 2018, p. 262).

**FinTech ecosystem**: According to Lee & Shin (2018, p. 37) there are five elements or dimensions that need to be considered to grasp the FinTech ecosystem: 1) The FinTech start-ups 2) the Technology developers 3) Government 4) Financial customers and 5) Traditional financial institutions.

**Information security**: according to ISO/IEC 27032:2012(E) Information security is presented as “the preservation of the confidentiality, integrity and availability of information”. The ISACA CSx cybersecurity Fundamentals Study Guide further elaborate on the connection between cybersecurity and information security. The Guide namely states that “in reality cybersecurity is part of information security”.

**Cybersecurity**: According to ISO/EIC 27032:2012 (E); cybersecurity is interpreted as “preservation of the confidentiality, integrity and availability of information in the Cyberspace”.

**IoT**: Internet of Things characterized by heterogenous technologies, which concur to the provisioning of innovative services in various applications domain, it is considered as the angular stone of the Information Communication Technology (ICT)market (Sicari et al., 2015, p. 146).

**TAM**: Davis (1989) developed the Technological Acceptance Model (TAM) by proposing that Perceived Usefulness, Perceived Ease of Use, behaviour and usage, influence a person a person’s intention to use new technologies.
2. Background and delineations

2.1 The FinTech’s ecosystem: dynamics and challenges

Different organizations have corroborated that the FinTech market activity had gained momentum by spreading geographically (PWC, 2017; KPMG, 2018). The investment forecasts estimated the FinTech industry to evolve from 3 billion to 8 billion USD in 2018 (Diemers et al., 2015 p. 4). The disruptive nature of FinTech puts in perspective its ability to challenge the current state of affairs by rattling the traditional financial institutions (Lee & Shin, 2018, p. 35). As we have previously mentioned, the threat of entry represented by FinTechs, forces existing financial actors to either develop internal capabilities or collaborate, in order to remain competitive (Lee & Shin, 2018, p. 35). As a result, a comprehensive understanding of the FinTech ecosystem is therefore essential to properly identify the different actors within industry and pinpoint not only its dynamics but also its challenges.

A first contribution to the FinTech ecosystem was suggested by Diemers et al. (2015, p. 5). Diemers et al (2015, p.5) regarded the environment has being governed by three parties: respectively entrepreneurs, governments and financial institutions (see Figure 1). According to Diemers et al. (2015, p. 5), each of the entities have a crucial role to play in order to nurture the ecosystem. On one side, the governments are eligible for implementing and pursuing the regulatory environment which will assist and promote entrepreneurial activity. On the other side, the financial institutions are defined as all financial institutions whether existing at the global or local level. Financial institutions should embrace a collaborative role with FinTech start-ups to strengthen their competitive edge (Diemers et al., 2015, p. 5). Lastly, entrepreneurs are shaping the ecosystem by providing solutions which are inventive and yet highly disruptive in regard to the financial industry.

![Figure 1. Major participants in the FinTech ecosystem. Source: Diemers et al. (2015, p. 5)](image)

Building on the first contribution by Diemers et al. (2015, p. 5), Lee and Shin (2018, p. 37) have identified within the FinTech ecosystem two more participants.

The two complementary participants suggested by Lee and Shin (2018, p. 37) are the technology developers and the financial customers. By financial customers, Lee and Shin (2018, p. 37) are dissociating end customers and organizations. The distinction made therefore supports the competitive dimension between the FinTech start-ups and traditional financial party. Their revised model of the FinTech ecosystem is exposed in Figure 2.

![FinTech ecosystem](image)

**Figure 2. FinTech ecosystem**

Source: Lee and Shin (2018, p. 37)

Nevertheless, both the financial Institutions and the FinTechs will be compelled to address the following matters in the years to come, since according to Lee and Shin (2018, p. 43) each of them will represent a challenge:

1) Investment management challenge.
2) Customer management challenge.
3) Regulation challenge.
4) Technology integration challenge.
5) Security and privacy challenge.
6) Risk management challenge.
Even though all of these challenges are mentioned by Lee and Shin (2018, p. 43), we have decided to elaborate only on the ones that are supporting our topic. We will be precisely investigating how the regulation challenge has promoted the security and privacy challenges which in themselves are affecting the technological acceptance of FinTech.

2.2 The Regulatory framework

The challenge we considered to be the most important is the regulation one. In fact, diving into the regulatory environment enables us to understand the reason why regulations are the catalyst to the FinTech phenomenon. The evolution of the financial industry is driven by the regulatory changes (Freij, 2018, p. 21).

According to Freij (2018, p. 22), the ongoing changes and future regulatory changes within the finance sector, represent the ultimate issue as they require time, investment and management. However, the regulation frame is both a source of challenge and opportunity. In this line, the first argument emphasized by Freij (2018, p. 22) is summarized by the prevailing importance and significance of the regulations onto the financial industry as they appeared to exponentially intensify by frequency and impact. To illustrate his point, Freij (2018, p. 22) made a comparative analysis of the twentieth century and twenty first century in terms of regulations. Freij’s conclusion underlined the time span discrepancies where regulations were formerly introduced slowly in contrast to today’s regulations characterized by “volume” and “complexity” (Freij, 2018, p. 23). In essence, the inevitable changes occurring at a higher pace in terms of consistency and significance led to disrupt and create a favourable regulatory environment currently driving innovation within the financial industry.

The financial crisis in 2008 not only created a regulatory aftermath but also had another drawback. The financial crisis in 2008 not only weakened the global financial system but also highly discredited the banking industry which was held responsible. The overexposure and use of financial derivatives led increase the risk due to the interconnectedness of the banking system, while the incapacity to deal with credit risks and operational risks taken gave the final blow.

As a result, major financial institutions went bankrupted, but the economical damaged which had been quantifiable begot another collateral damage: both their brand image and identity have been affected resulting in decreasing the notion of trust in the eyes of their customers. In this continuation, the decline in credibility and trust encountered by the traditional banks created a consumer behaviour shift where customers are now keen to experience innovative alternative to the traditional financial service providers (FSR, 2016, p. 86). Innovation which is conveyed and seized by FinTech’s and their ability to innovate through disintermediation; by proposing tailored technologically driven solutions responding to undermined consumer’s needs. Lee and Shin (2018, p. 37) on top of arguing for the centre role of the FinTech start-ups, also expressed the consumer behaviour change due to the increased range of options given by FinTech’s solutions. Today’s consumers are considered to be more open minded and responsive to change, which eventually leads to redefine the customer experience and their attitude.
Beforehand consumers were accustomed to solely use one service provider, while today’s changing environment offered them access to a wider range of options thereby emphasizing their appetite and interest for a complementary/combination of service providers (Lee & Shin, 2018, p. 37). The overall finding is highlighted through the drastic undergoing changes within the financial industry where the disruptive nature of the FinTech movement disputes the traditional financial industry and its products by revolutionizing the areas from payments to investments. More recently, the regulatory environment proposed directives such as Payment services directive 1 (PSD1) and Payment service directive 2 (PSD2). These directives defined what a payment service provider is and helped FinTechs to propose innovative financial solutions based on existing financial data by allowing third parties to have access to customer’s bank accounts (Nicoletti, 2017, p. 201).

In conclusion, the regulatory environment is stimulating innovation within the financial industry. The distinct changes which concurrently arose to the extent the exponential increase in terms of volume and complexity of today’s regulations, the inefficient implementation of these regulations as well as the credibility decline of traditional financial institutions; led to generate an appropriate environment for FinTech’s and their innovations. The tension between promotion and regulation outlines the relationship between compliance, innovation and data security challenges. It is precisely the data security challenge that we intend to further scrutinize in the next section.

2.3 Information security challenge

2.3.1 Context

One of the FinTech challenges which have been addressed gained a lot of scrutiny in the recent years not only due to its controversial aspect but also because of its repercussions on the global scene. Media coverages highly contributed to shed the light on a particular issue through the 2013 Snowden allegations. Snowden’s public whistleblowing raised the question of information security and data privacy. The major incident led to create growing concerns about information security and notably within the finance industry. According to the 2018 Data Breach Investigations Report published by Verizon (Verizon, 2018, p. 4), there have been over 53,000 information security related incidents and 2,216 confirmed data breaches. The report elaborates by specifying that 58 % of the incidents targeted small businesses.

In fact, the industry, which is the most exposed to information security incidents, is the financial industry. Reports are formal; due to the nature of the business traditional financial service providers are dealing with, and considering the value of the information, any finance related industry is at stake. Cyber criminality is taking many forms; the most common one is targeting web application authentication processes. The reasons which motivated these attacks were diverse, nevertheless 93 % of them were financially driven and 5 % were industrial espionage. Out of the different data breaches, the information which was stolen was 36 % individual related, 36 % payment transactions data, and 13 % bank related (Verizon, 2018). The recurrence of these incidents contributes to an environment where a Damocles sword hangs above each and single one financial institutions or financial related business. Additionally, to the threat of a cyber-attack, the consequences could be devastating as leakages would inevitable tarnish the financial institution’s reputation and credibility.
Resulting from the plausible incident, any institution would be entitled to create a crisis unit capable of handling the situation by shutting down the system quickly and spend the resources needed on legal guidance, forensics investigations to avoid similar events. Nowadays with the changing regulatory environment, the General Data Protection Regulation (GDPR) voted in 2016 will become operative and will result in turning the information security challenge as part of the risk management. The noncompliance with the GDPR requirements will be penalized, moreover each data leak or privacy violation will potentially result in fine accounting up to 4% of the annual global turnover or 20 Million EUR, whichever is higher (Kryparos, 2018, p. 48).

2.3.2 FinTech and Information Security

Even though the changing regulatory environment acted first as a catalyst by promoting the FinTech phenomenon into the spotlight, it inherently touched upon one of the prominent challenges of “FinTech”: to the extent Information Security. The information security becomes of even greater prominence due to the nature of the business that FinTechs are involved in. The first argument eventually relies on the fact that FinTechs are dealing with the financial industry where they enter the environment as non-traditional services providers. The second argument relies upon the business model characteristics of FinTechs. FinTechs are entitled to always be available as it represents not only the core of their business but also the reason of their existence (Kryparos, 2018, p. 48). However, there is one existential dilemma between being “Always available” yet secure. The expression “Always available” incarnates an explicit promise made by FinTechs, which is yet disputed by cyber criminality. The old-fashioned view of achieving security relied on security through obscurity, where isolation and limited access were extolled.

With the rise of Internet, this “security through obscurity” strategy appears to be highly delusional and no longer feasible in an environment where both open network and web technologies takes the front (Kryparos, p. 47). These features fully embraced by the FinTechs reaffirm the existing tension between the solutions promoted and the challenges they are facing. FinTechs are able to provide solutions which are tapping into the customer needs which were so far undermined by traditional financial institutions (Kryparos, 2018, p. 43).

Howbeit, the problem which arouse by enabling the simplification of the customer experience, is that the entire attention has shifted to the customer side which eventually echoed for the FinTechs to ensure a viable solution to the “availability” and “security” paradigm. The solutions need to be available, secure by design and yet customer friendly (Kryparos, 2018, p. 47). In parallel, the notion of Time to market especially within the FinTech ecosystem is a crucial determinant to outrun the competition (Kahn 2005, cited Kryparos, p. 49). The solution is required to simultaneously answer to a real-life problem, bear in mind the consumer needs and finally be delivered with the optimum timing. The complexity of the demands could have the opposite effect, as outrunning the competition may lead to cutting corners. Cutting orders here simply means choosing the fastest way to reach one’s goal, and within the FinTech ecosystem it would be interpreted as launching a product or service without ensuring its security. The lack of security would inadvertently damage the company and raise question the continuation of the organization as going concern.
It is not important whether the problem occurs now or later on, the real problem is the statement made which is corresponding to a gamble where the organization who did not consider securing its product/services, put at stakes its life expectancy. A parallelism has been drawn between information security and racing cars. The analogy is developed the following way, a racing car has to be fastest possible to beat its contenders, and in the meantime, speed is only made possible by the car’s possibility to brake. The need for brakes thereby supports the ultimate goal of being fast. Bearing this information in mind and applying it to a FinTech context, it is likely that information security and its rules will allow sustainability. Notwithstanding, the growing concern for time to market and speed gave birth to a new type of software development known as agile manifesto. The agile manifesto extols 12 principles which are made to facilitate the software development by addressing different touchpoints (Fowler & Highsmith, 2001).

One of the recurring notions that are stressed within the agile manifesto is the time interval at which the software needs to be delivered to the customers. Apart from providing a utopic ideal of software development, the practice often revealed that even though the manifesto promotes cooperation and speed and autonomy; it is most likely that the people involved are losing track of the whole context. As mentioned by Kryparos (2018, p. 50), the problem derives from the principles themselves, to the extent the objective of frequent interval delivery involves selecting features and matching the customer needs. The hierarchy implicitly imposed by the principles, often results in comparing different features, their direct utilities and the complexity they require to be produced. The outcome thereby is altered by the individuals that are in charge of developing the software. Undoubtedly few individuals are acknowledging the direct impacts of sustainability, legal compliance or even security (Kryparos, 2018, p. 50). Once again, information security is undermined and every time technical security vulnerability occurs, the public needs to be advised to upgrade to the newest software version. These technical failures are not well perceived by the public which categorized them as the cause of the security problem instead of the symptoms (Kryparos, 2018, p. 52).

The reality is that the cause is not the technology but the processes, the protocols and individuals behind the technology who need to be held responsible. The shortcuts taken by the people in charge are hurting their daily businesses as the security within the solutions provided are not robust enough. Consequently, the rapid launch of non-robust solutions onto the market to simply benefit from the precursor advantage, have many downsides such as discrediting the technology proposed (i.e. loss of customers credibility), provoking brand reputation damage and lastly creating a “technical debt” for the company (Kryparos, 2018, p. 52). A technical debt is represented by the non-consideration of recurring issues which will eventually create a core problem during the future software development, thereby increasing the complexity. In other words, it would be like building a house on sand instead of rock.
In the previous section, we mentioned that FinTechs are exposed to a dilemma: available yet secure. Nevertheless, the inclusion and development of information security within the software process is undermined as time to market and need for speed is preferred. The rush for being the precursor often leads to a “technical debt”, highly difficult to correct in the later stage of software development. The numerous observations confirm the need to study information security within the FinTech context. In the next section, we will precisely define how cybersecurity and information security interacts.

2.3.3 Cybersecurity and Information Security: commonality and delineation

It has been formerly mentioned that cyber criminality has gained a lot of attention in the recent years, notably in regard to the various incidents which occurred at the international scene. The emergence of cyber criminality has thus induced another problematic portrayed by the ongoing discussions about the definition and delineation between the following terms: cybersecurity and information security. In this line, Von Solms and Von Solms (2018), communicated on the subject by wondering “what goes where”. In order to provide and ground-based argumentation, the two scholars sought out to enlighten the commonalities and delineations of these two words. Von Solms and Von Solms (2018, p. 5) purposively selected two well-known sources to strengthen their argumentation. Cybersecurity is consequently defined based on ISO/IEC 27032:2012 and the ISACA CSx Cybersecurity Fundamentals Study Guide. According to the first source namely ISO/EIC 27032:2012; cybersecurity is interpreted as “preservation of the confidentiality, integrity and availability of information in the Cyberspace”.

In parallel, information security is presented as “the preservation of the confidentiality, integrity and availability of information” (ISO/IEC 27032:2012(E)). Subsequently the main delineation resides in the contextualization where on one hand cyber criminality is enclosed in the cyberspace while information security is “omnipresent”. The definitions thereby provide the point of departure of the scholar’s interpretation. In this perspective Von Solms and Von Solms (2018, p. 5) mentioned the ISACA CSx cybersecurity Fundamentals Study Guide to further elaborate on the connection between cybersecurity and information security. The Guide namely states that “in reality cybersecurity is part of information security”.

Furthermore, Von Solms and Von Solms (2018, p. 5) compared the terms and highlighted that based on ISACA CSx cybersecurity Fundamentals Study Guide, information security englobes all type of information while in contrast cybersecurity is concerned with the protection of the digital assets. To the extent, digital assets comprise the totality of assets whether material or immaterial. The inclusion of the dual dimension allows taking into consideration the protection of physical installation (networks, hardware) and the information processed traveling thanks to the interconnected networks.
Figure 3. Relationship between cybersecurity and other security domains.
Source: Von Solms and Von Solms (2018, p. 5).

As the results of the two former points, cybersecurity is presented by Von Solms and Von Solms (2018, p. 6) as a component of information security, as in Figure 3. The latest assumption clarifies the following aspects: information security deals with the overall information and comprises cybersecurity which is narrowed to the protection of the digital assets. Furthermore, the main domain into which cybersecurity applies is the “internetworked information systems” which simply refers to the Internet. Once the terminologies have been defined it facilitates the discussion around their application. The application inherently touches upon the notion of governance, as the ISO/IEC 27014:2013 that the governance surrounding the information security refers to the “system by which an organization’s security activities are directed and controlled”. In conclusion the information security governance is the governance of the information regardless of its forms (Von Solms & Von Solms, 2018, p. 6).

Extending on the governance matter from a cybersecurity perspective, cybersecurity governance could be categorized as part of the information security governance and represents the process of directing and monitoring the protection of the digital information assets from the risks arising from the use of the Internet of Things (Von Solms & Von Solms, 2018, p. 6). The ultimate point reasserts that the risk derives from the main domain into which operates cybersecurity which is Internet. Nevertheless, the definitions highlighted have not been expressed in regard to the specific context we are interested in. Therefore, the next section will elaborate by further developing the forms that cybersecurity takes from a FinTech perspective.

2.3.4 Cybersecurity within FinTech

According to Gai et al (2018, p. 263), who elaborated on the cybersecurity notion, provided a mapping of the different issues that FinTechs are facing. One the ongoing issue which has been pinpointed by Gai et al. (2018, p. 263) is the security and privacy ones.
The scholars have regrouped and narrowed the security and privacy issues into three dimensions including 1) Business operations 2) Outsourcing 3) Financial privacy. The first concerns preoccupying the financial industry used to solely be a matter of business operations.

However, the different incidents permitted to create an incident classification and a better understanding of the reasons why they occurred. The incidents remained complexed to analyse and interpret in order to build a strategy (Gai et al., 2018, p. 263). The only affirmation that can be made is that two elements appeared to be crucial in order to secure electronical transactions, particularly perceiving the privacy concerns and building up a trust mechanism (Liao et al., 2011 cited in Gai et al., 2018, p. 263). The question is how can one build a “trust mechanism”? The underlying interrogation thereby addresses the practicalities behind the cybersecurity dimension. Thanks to Von Solms & Von Solms (2018), we have emphasized the main domain of cybersecurity namely “internetworked information systems”. Von Solms & Von Solms (2018) later underlined that the expression merely referred to Internet. We thereby extend what Von Solms and Solms (2018) formerly expressed by prolonging Internet to Internet of Things (IoT).

According to Gai et al (2018, p. 264), the only way of solving the security risk and building a trust mechanism is therefore to either develop a physical method or an application-based method (Gai et al., 2018, p. 264). The next section will investigate in detail another concept intimately linked to the information security one, namely trust.

2.4 Trust and traditional finance

Besides the economic damage, the financial crisis in 2008 brought out another perspective into play: to the extent the collateral damage has been its repercussion onto the financial system. In essence, the quasi pontiff reign of the “Financial Institution” was weakened and its supremacy, authority and knowledge implicitly contested. The unquantifiable disturbance concurred to question the financial institution’s brand identity and image. The institution which formerly appeared to exhibit and extol qualities like credibility, stability and trust yet appeared to have lost control. The disclosure of highly exposed positions through the use of derivatives intrinsically created a considerable wave of panic amongst investors thereby creating the aftermath medias relayed. The substantial loss of credibility and thus trust encountered by the traditional financial service providers participated in shifting the consumer trust and behaviour. It is precisely in this context that the FinTech phenomenon gained momentum with regulations as its main catalyst.

The growing phenomenon entered the financial industry as a non-traditional finance provider, proposing to consumers an alternative; conveying innovation and addressing needs which were formerly dismissed by traditional institutions. On one side the traditional finance industry is engaging in a transitional stage intended to gain back the trust lost. On the other side, FinTechs face a considerable challenge in ensuring a solution combining features such as “availability” and “security”. The concept of Trust once again appears to be of importance, as it may be the answer to the consumer’s concerns about adopting the new technological breakthrough. Nevertheless, what is actually trust? And why trust appears to be vital for FinTechs?
These are the interrogations we will investigate in this section. The underlying nod
while investigating the concept of Trust is potentially the excess of definitions within
the academic literature firstly reasserting the importance yet complexity of the former
element and current lack of agreement amongst scholars. As mentioned by Beldad et al.
(2010, p. 858), there is no universal definition of Trust, rendering the concept highly
intricate to define. Nevertheless, the first element which is considered to define trust is
the process it involves, namely highlighting its bilateralism. According to Lee and
Turban (2001, p. 76), one of the roots of the disagreements within the trust literature is
the failure to consider the trusting party and the party to be trusted.

Despite the abundance in terms of definition it appears that the field is characterized by
a two-way stream: the first one regards trust as an expectation regarding the behaviour
of the interacted partner (Barber 1983, Koller 1988), the second one in comparison
regards trust as ability or acceptance to exposure to vulnerability (Doney et al., 1998).
The importance of trust in different fields is unquestionable yet the disciplinary
approaches onto the construct heavily influence its definition. Regarding the concept of
Trust from three different perspectives might elucidate some of its conceptualizations.

2.4.1 Trust conceptualizations

a. Personality theory

The first conceptualization is mostly referred to as personality theory; to the extent this
perspective interprets trust from a psychological perspective (Lee & Turban, 2001, p.
77). As a result, the individual and its attributes are at the core of the trust construct, as
it is argued that trust originates from the individual’s personality. Trust is thus a
psychological state which could be constructed from the various mechanical influences
of the environment or beliefs, values and emotions (Beldad et al., 2010, p. 858). In
essence, this theory argues that individuals may have different propensities to trust
which depend on their personality and own development experiences, or cultural
background.

b. Risk expectations theory

The second perspective addressed by the literature is trust as an expectation where the
emphasis is given to the sociological function of trust instead of the psychological one.
As argued by Blau (1964), trust is to be a crucial feature in both the introduction and
maintenance of social relations thereby creating stability yet trust through exchanged
obligations. In this regard, trust is perceived both from a psychological and sociological
perspective. The implication of a socio economical perspective onto the concept of trust
is thereby shaping the trust expectations of the individual involved in the interaction.

Barber (1983) expressed three types of expectations resulting from trust which he
described as 1) expectation of persistence and maintenance of social order 2)
expectation of the technically competent role performance from those involved in
individuals’ social relationships and lastly 3) expectation that participants within the
interaction will execute their economic and moral obligations or responsibilities.
The second line of theory puts in perspective the trustor and trustee relationships by literally challenging the trustor’s perception of the trustee, to the extent whether the trustee is honest with dealing with what it is intended to do, regardless of the materiality of the good.

The paradox here is the self-projection of trustworthiness of the trustor towards the trustee, which intrinsically pinpoints that trust, is partially appraised by the trustor ability to assess the reliability of the trustee. As the trust is apprehended from a transactional perspective, since it is involving a linkage between trustors and trustees, it includes dimensions such as reputation, performance and appearance (Sztompa, 1999). The second perspective on trust also comprises another element, which is intimately linked to the expectation attribute. In fact, as mentioned by Zand (1972, p. 230) people who trust automatically concede part of their power to the other party, thus increasing their exposure to vulnerability by putting themselves into a situation they cannot control. In all forms of exchanges, there are ultimately uncertainties reasserting that risk creeps underneath and that accepting to trust implicitly means accepting dealing with the risk of being vulnerable (Beldad et al, 2010, p. 859). The former element pinpoints an interesting dilemma by questioning whether one trust because of the exposure to risk or does one take risk because of trust? Depending on the viewpoint there might be different inferences which could be withdrawn. The first conclusion would emphasize that risks determine trust, while the alternative would conceive trust as the antecedent of risk-taking behaviours. The latest touches upon another dilemma within the conceptualization of trust which is portrayed not by the interaction between trustor and trustee, but whether each of the participants is acting in a rational or irrational way.

c Institutional theory

The last perspective on trust emerges from the consideration of both sociological and economic implications. The first element within this conceptualization is to view trust from a collective perspective instead from isolated individuals. If trust is contended from a collective perspective, it allows applying trust to the relations amongst individuals instead of relying on their psychological states (Lewis & Weirget, 1985, p. 968). The social human interactions are founded on the notion of exchange whether in the form of material or immaterial goods (Blau, 1964). Along this line, Blau (1964, p. 91) further elaborated that social exchange is primarily motivated by individuals and their willingness to voluntarily engage in a relation justified by the expected return they bring. Nevertheless, the expected return or benefits in a social exchange is not fully defined, which is the reason why economic and social exchanges differ. The economic exchange is usually grounded in a formal contract while the social one is informal and not fully depicted. Even though economic and social exchanges may differ due to their nature, the commonality between them is that they both imply trust for either the continuation or completion of the exchange (James, 2002, p. 293). The last element which is highlighted by the notion of trust within social exchanges is the dependency between its actors. The dependency emanates from the fact that individual’s needs may require the intervention of others who are likely to meet their expectations. However, the commitment from one party to another depends on trust.
The penultimate delineation corroborated by the trust’s conceptualization from a sociological and economic perspective, is based on its collective attribute. Viewing trust as an institutional phenomenon broadens the trust interactions. In other words, trust is no longer defined as singularly describing an interpersonal exchange but could represent an individual interaction with a group, organization or institutions (Lewiki & Bunker, 1996, p. 119). Thereupon trust could be defined as the reliance of one protagonist upon an established duty ensured by another party seeking to protect and acknowledge the rights and interests of all the parties engaged (Hosmer, 1995, p. 393).

2.4.2 Institutional trust and bank crisis

The first trust which has been undermined by the financial crisis in 2008 is the trust that individuals grounded into the institutions. It is precisely the consideration of this perspective which helps us to comprehend how the financial system and specially the banking industry failed to complete and continue the trust it has built. Individuals had engaged in economic exchanges with the banking industry thus expecting the banking industry to perform as promised. The implicit implications anchored in the economic exchanges, led individuals to feel deceived. The banking industry failed to meet people’s fiduciary and moral obligations. In essence, the risky position whether in the form of credit risks, or derivatives led investors to think that the banking industry, which was supposed to also maintain the social order, had failed. As the scandal was revealed, trust given to traditional financial service providers decreased. Moreover, the mistrust resulting from the financial crisis impacted the customer loyalty, as individuals now need to reassess their willingness to accept the risks of engaging in a situation which they cannot control.

As mentioned by Kryparos (2018, p. 43) trust within the financial institutions has been supported and built over years of consistency in delivering promises while ensuring the customer’s interests. The trust was then expressed in terms of credibility given to the companies capable of exhibiting transparency about the products and services it offers (Lewan, 2018, p. 111). In conclusion, trust within the financial industry is extended to the notion of security. Trust is corroborated by the notion of security, and especially due to the nature of the exchange. The two parties involved in the exchange, are not only mutually agreeing on fiduciary implications but also moral ones. In the financial industry trust is also often connected to security, since customers give their money to banks with the demand that no one is stealing or misusing the money (Lewan, 2018, p. 114). Additionally, according to Danny Aerts, CEO at IIS (Lewan, 2018, p. 122), security is the conception of trust that will emerge more and more in the light of the different cybersecurity incidents, reasserting that it has become easier and cheaper to cause harm to the financial industry which is the most exposed industry.

We have so far contextualized trust within the financial crisis, and its implications at the institutional and individual level by elaborating and characterizing the different levels of trust which have been affected negatively. In conclusion the former role of the Banking industry which is maintaining a certain order while embodying the technical yet competent attributes of ensuring the expectations of individuals; had failed. The mistrust created, led individuals which were engaged in social and economic transactions to doubt the institution’s ability to perform their fiduciary and moral obligations thereby comforting individuals that their interests were no longer the priority.
The loss of credibility in the form of trust firstly reasserted that within the financial industry trust and security are two constructs interrelated, but mostly that trust is at the core of the engagement, continuation or completion of exchanges whether social or economic.

2.4.3 FinTech: Offline and Online trust.

By regarding trust as of importance within exchanges and within the financial industry, we infer that trust would also be of importance for FinTechs. In order to argue in this direction, we will further elaborate between the determinants of trust in the light of FinTech’s business models, namely by considering the trust determinants between offline and online.

The underlying interrogation here is to question the materiality within the trust phenomenon, in other words pinpointing if trust differs between offline to online experiences. Online trust has been defined from a psycho sociological perspective, characterized by a confident attitude towards an online situation of risk where one’s vulnerability will not be used (Corritore et al., 2003, p. 740). Does trust diverge between the physical and the online world? The answer is straightforward, as it is argued that the common denominator between the two is their rootedness on exchange. As in the offline interactions, the trustee has to present itself as trustworthy. The major difference between offline and online trust is argued by Shankar et al. (2002, p. 327) to be the scope of trust where on one hand the object of trust is often an individual (or group of individuals such as organization etc) while on the other hand the trust is based not only on the mean of exchange but also the organization deploying the technology. It is precisely the online trust perspective which is of crucial importance for FinTechs. FinTechs are innovating thus providing a new customer experience supported by technologically driven solutions. The reliance on innovation through technology for FinTechs corroborates the definition of online trust, where both the technology and organization deploying the technology matter. The technological aspect raises the question whether the platform proposed is trustworthy for the individual. The organizational aspect concurs whether the organization or in our case FinTechs are perceived as trustworthy. FinTechs are facing a current challenge, which is to exhibit trust (Kryparos, 2018, p. 45). FinTechs need build trust from an institutional perspective by creating trust in the technology they provide.

In fact, FinTechs have not existed long enough to benefit from customer loyalty as the traditional financial institutions did. As a non-traditional financial provider, FinTechs could benefit from the decline of credibility within the traditional financial industry to lock on the customers who were deceived. The online trust literature provides extensive insights into the potential antecedents of trust. To name a few there are the Perceived Ease of Use (ergonomic), the information quality, the graphical characteristics, the social presence cues, the customization and lastly the privacy insurances and security (Beldad et al., 2010, p. 861). The last antecedent (i.e. security) is argued to be the most important one for FinTechs as they are dealing with confidential and financial information, which needs to be secured at all time. FinTechs need to focus on the trust that is created through their capability to ensure the integrity of the customers’ money and data (Kryparos, 2018, p. 43). As we have mentioned earlier the only way of solving the security risk and building a trust mechanism is therefore to either develop a physical methods or an application based method (Gai et al., 2018, p. 264).
The various incidents and threats that represent cyber criminality heavily modified the regulatory environment by specifically addressing within the new directives the security challenge for instance the GDPR regulation. Consequently, any business related to the financial industry is at stake and should consider information security as a new dimension of their risk management strategy.

In this regard, FinTechs are even more exposed to the threat due to the nature of their business which relies on providing technological financial solutions that need to be available and yet secure. The dualism existing between availability and security requires a high level of trust. Nowadays internet services enjoy a high degree of trust although it is a recent phenomenon compared to other industries. No one questions the integrity of for example amazon and almost everyone is willing to buy things online nowadays (Lewan, 2018, p. 117).

Nonetheless social or economic exchanges imply at least two participants in the form of the trustee and trustor. This process also accounts for the last issue regarding FinTechs, namely symbolized by the trust they need to have with the party using their solutions. The regulatory environment demands new criteria both from banks and FinTechs, as the Know your customer (KYC) is growing (Lewan, 2018, p. 117).

In conclusion, the only way for FinTechs to build a trust mechanism is to solve the risks either physically or from a web application method (Gai et al., 2018, p. 264). The information security and trust dimensions thereby touch upon two major facets which are highly relevant for FinTechs due to the modernity of the phenomenon, and the challenges they depict for the innovation and its technological acceptance.
3. Theoretical background and Literature review

3.1 Theory of Reasoned Action (TRA)

As we have formerly expressed, the complexity depicting the FinTech phenomenon results from the duality between two features: namely “security” and “availability”. To the extent, the duality extends to portray the FinTech’s penultimate challenge which is the need to build a trust mechanism while ensuring security. Ensuring security and trust is perceived to be one of the reasons why consumers are reluctant to shift to the non-traditional financial service provider. Consequently, the presupposed interrelation between information security and trust in the context of FinTech could constitute the solution for promoting technological acceptance amongst consumers. In this line of argument, technological acceptance depicts the ultimate challenge for FinTechs.

There are multiple theories addressing the topic of technological acceptance within the literature. Even though not all the theories are using the terminology “technological acceptance”, most of them approach the topic by investigating the field of consumer behavior in relation to technologies. For instance, one of the precursors is Ajzen and Fishbein (1980, p. 4) who proposed the Theory of Reasoned Action (TRA). TRA aimed to study the components affecting the individual’s conduct in relation to technologies. The Theory of Reasoned Action (TRA) develops a single theoretical framework constructed on various preconceptions about the individual (Stewart & Jürjens, 2018, p. 113). The first prerequisite simultaneously acknowledges the implications of behavior and subjectivity onto the individual’s intention to use a technology. In essence, the Theory of Reasoned Action (TRA) contextualizes behavioral intention as stemming from the link between individual’s attitude and subjective implications (Stewart & Jürjens, 2018, p. 113). The subjective attribute within TRA, describes the effect of someone’s expectations onto the individual’s intention. To the extent, it represents the individual’s recognition of the social norm as influencing its own behavior (Ajzen & Fishbein, 1977, p. 7).

In conclusion, the theory’s foundation also represents its limitations. We note three elements which we believe do not support TRA regarding FinTechs. First of all, TRA is highly centered onto the individual and its personal attitude towards behavior. Ajzen and Fishbein (1980) mentioned that if the individual exhibits a positive attitude towards a specific behavior, he/she is more likely to perform the behavior. Secondly, we believe that this specific implication may highlight to perceive trust within TRA from a personality trait perspective. Trust would thus be characterized by the individual’s propensity to trust based on its previous experiences (Mayer et al., 1995, p. 715).

Subsequently, trust would be solely attributed to the individual features and thereby not applicable in the context of FinTech where we hitherto expressed the need to consider trust in relation to FinTech’s context: namely in terms of online trust. Thirdly, the technologies examined are too far from the one promoted by the FinTech’s phenomenon. In fact, what could be influencing previous technologies may not be applicable to FinTech as it may neglect important dimensions for instance security and trust.
3.2 Technological Acceptance Model (TAM)

The second theory identified is Technological Acceptance Model (TAM). The theory has been originally proposed by Davis (1989). Davis (1989, p. 319) realized the lack of conceptual modellings identifying the antecedents of user acceptance in regard to information technology. Davis (1989) aimed to figure out what was causing individuals to either accept or reject novel information technologies. Davis (1989) formulated that technological acceptance relies on two antecedents: “Perceived Usefulness” and “Perceived Ease of Use”.

“Perceived Usefulness” is characterizing the individual’s propensity to believe that using a specific system would improve job performance (Davis, 1989, p. 320). The second variable describes to what degree a person believes that using the new information technology would be effortless (Davis, 1989, p. 320). According to Yang (2004, p. 260), TAM is perceived to be the most widely used and one of the best models to investigate various individuals in relation to technological adoption. Along this line, Venkatesh and Davis (2000, p. 186) argued for the convenience of TAM by indicating that it could be combined with alternative models; such as the Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB). Later, Venkatesh & Davis (2000, p. 186) extended the TAM by creating the TAM2. TAM2 is supposed to correct the deficiencies and limitations of the original TAM. In essence, the TAM2 incorporated two additional dimensions represented by: social impact and cognitive procedures (Stewart & Jürjens, 2018, p. 114).

The additional determinants helped to further understand that technological acceptance may vary as the user become more experienced with the technology. The new determinants integrate theoretical constructs about social influence processes such as subjective norm, voluntariness, and image, and cognitive instrumental processes such as job relevance, output quality, result demonstrability and Perceived Ease of Use (Venkatesh & Davis, 2000, p.187). Bearing this in mind, we believe that TAM as originally constructed, is not directly applicable to the scope of our study. The TAM conceptualization stresses out technological benefits defined as “usefulness” and “ease” while undermining the impact of technological disadvantages. Furthermore, we also believe that the TAM2 is not fully applicable to the scope of our study, in the sense that the corrections still fail to take into consideration the impact of the necessary dimensions that are information security and trust. As a result, we argue that a revision of the TAM is needed in order to fit the FinTech’s ecosystem and its challenges.

3.3 Extended Post Acceptance Model (EPAM)

The third theory identified consists of the combination of two theories that are the expectation confirmation theory (ECT) and post acceptance model (PAM). Lim et al., (2018, p. 1) proposed the extended post acceptance model (EPAM). The model is seeking out to explain user’s post adoption behavior about new information technology. As mentioned above, EPAM stems from the combination of ECT and PAM. The expectation confirmation theory (ECT) is referred to a longitudinal model primarily used to scrutinize the potential variance between two periods: pre consumption and post consumption (Oliver 1981; Lim et al., 2018; p. 3). In other words, consumer’s intention to repurchase is imposed by their degree of satisfaction regarding the product or service used (Oliver, 1981, p. 28).
Later, Bhattacherjee (2001, p. 351) proposed based on ECT, a post acceptance model in order to better understand the information system continuance to use online banking services. As such, Lim et al., (2018, p. 5) decided to adapt ECT and PAM under an overarching framework by considering the factor’s that would be meaningful in the light of FinTech mobile payment services. EPAM is thus constructed around two factors: FinTech service knowledge and Perceived security (Lim et al., 2018, p. 3).

The first element defines knowledge as user’s understanding and utilization of information technology (Lim et al., 2018, p. 4). The second element categorized perceived security into service security, platform security, network security, and device security (Lim et al., 2018, p. 6). Different elements are of interest in relation to EPAM. First, it is one of the few studies that are actually considering information technology from a FinTech perspective. Secondly, the scope of the study also matches our intention for this thesis, to the extent the study of the FinTech mobile payments. Lastly, Lim et al., (2018, p. 2) thanks to EPAM analyzed how user’s knowledge and perceived security explain the persistence of mobile FinTech service payments. Consequently, EPAM reasserts the importance of perceived security dimension in relation the study of FinTech. Yet, the timeframes implications grounded in both the ECT and PAM and also present in EPAM do not support the use of this model in our study (i.e. longitudinal dimension in comparison to cross sectional aim in our thesis). However, the consideration and conceptualization of perceived security as a multidimensional construct is valuable.

3.4 Unified Theory of Acceptance and Use of Technology (UTAUT)

Finally, Venkatesh et al. (2003, p. 426) proposed a model aimed at unifying and integrating numerous models addressing the acceptance of information technology. The Unified theory of acceptance and use of technology (UTAUT) is stemming from the review of eight theories namely the Theory of Reasoned Action, the Technology Acceptance Model, the Motivational Model, the Theory of Planned Behavior, a model combining the Technology Acceptance Model and the Theory of Planned Behavior, the model of PC utilization, the Innovation Diffusion Theory, and the Social Cognitive Theory (Venkatesh et al., 2003, p. 425). The review of the theories led to highlight the eight dimensions which appeared to be of importance: performance expectancy, effort expectancy, attitude towards technology, social influence, facilitating conditions, self-efficacy, anxiety, and behavioral intention to use the system. UTAUT’s willingness to englobe so many different theories and attributes is too complexed and not matching the scope of our study.

3.5 Conceptual model and argumentation

In the light of the existing socio psychological theories addressing the topic of technological acceptance, the Technological Acceptance Model originally proposed by Davis (1989) has been confirmed as the most powerful and extensively used in various technological contexts (Lim et al., 2018, p. 2). Yet, the technological studies focused on the adoption of new technology in terms of pre-acceptance promotion and post-adoption (Lim et al., 2018, p. 2).
Despite the extensive application of TAM within the literature, few studies have actively investigated the acceptance of internet banking (Wang et al., 2003, p. 504). The advent of digitalization and the emergence of the FinTech phenomenon therefore provide a novel context to the study of technological acceptance. Although, there is a wide range of literature investigating either the processes or techniques used to effectively accept the adoption of FinTech, Stewart and Jürjens (2018, p. 113) mentioned the lack of a complete model illustrating the FinTech phenomenon.

TAM postulates that user adoption of new information is firstly governed by the user’s belief about the system. Nonetheless, we believe and support scholars who argued about the deficiencies about the TAM as not being universally applicable (Venkatesh & Davis, 2000). The acknowledgement of the deficiencies led Venkatesh and Davis (2000) to further develop TAM by considering both the social impact and cognitive procedures as mere elements of information system usage and adoption.

Additionally, the original TAM model over emphasizes the Perceived Usefulness (U) and the Perceived Ease of Use (E) thereby neglecting the constraints which might be undermining the utilization of information systems. As a result, technological acceptance is mostly defined in terms of perceived benefits instead of also recognizing the perceived risks. Furthermore, TAM has been questioned within the context of mobile banking services (Liu et al., 2009). The fact that TAM has been criticized regarding its applicability in the context of mobile banking reasserts one of the reasons why among the numerous emerging technologies we have decided to focus on one specific area of FinTech services, to the extent mobile payment.

In fact, due to the recent provision of ICT such as IoT both traditional and nontraditional financial service providers are proposing enhanced financial services. Mobile payment services are one of the most popular. The second argument for selecting mobile payment relies on a consumer perspective. Consumers acknowledge the user-friendly attribute of the services and use mobile FinTech services provided by non-financial organizations. Corporations such as Apple or even Samsung have for instance greatly participated in the transformation of personal financial services using emerging technologies (Lim et al., 2018, p. 2).

Consequently, we argue in the line of Stewart and Jürjens (2018, p. 113) who explicitly indicated the need to: “highlight the necessary perspectives for the FinTech adoption process”. We therefore assert the need to include two dimensions of high significance for the FinTech phenomenon: namely the impact of information security and trust onto the technological acceptance. Scholars have mentioned that information security and trust appeared to be crucial for FinTechs (Liao et al., 2011 cited in Gai et al., 2018, p. 263). Plus, different studies have outlined the importance of either security or trust in respect to technological adoption (Wang et al., 2003; Luarn & Lin, 2005; Liu et al; 2009; Liao et al., 2011 cited in Gai et al., 2018; Stewart & Jürjens, 2018).

The main distinction with prior researches is thereby postulated by the conceptualization of the information security and trust constructs. As we have briefly exposed, the original TAM model intrinsically provides a subjective comprehension of the technological acceptance as merely including perceived benefits (Venkastesh & Davis, 2000).
To further elaborate on the Technological Acceptance Model (TAM), we have decided to implement the dimension of security and trust where we settled to adapt the model of Stewart and Jürjens (2018) by defining their variable “Data Security” and “Customer Trust” differently. Before exposing our conceptualization of Stewart and Jürjens (2018), we will briefly present the dimensions on which we agree on. Stewart and Jürjens (2018) proposed the dimension Value Added (VA) as including Perceived Ease of Use (E), and Perceived Usefulness (U). We share the same opinion as Stewart and Jürjens (2018, p. 115) who mentioned that (E) and (U) represent the internal and external elements influencing FinTech’s adoption. Moreover, Stewart and Jürjens (2018) believed that the construct of Trust and Security should be studied in the context of usability.

In fact, the scholars relied on Clark (2002) and Landford (2006) who postulated that User Design Interface needs to be considered in relation to security. Additionally, the online trust literature supports User Design Interface (UI) as an antecedent of trust (Beldad et al., 2010, p. 861). Lastly Stewart and Jürjens (2018) included the FinTech Promotion dimension (FP) as being promoted by Value Added (VA), User Design Interface (UI), Data Security (DS) and Customer Trust (CT). In other words, they are the antecedents affecting the behavioral customer’s intention to adopt FinTech services (Stewart & Jürjens, 2018; p. 114, Beldad et al., 2010, pp. 861-867).

The first issue with Stewart and Jürjens (2018) conceptualization of “Data Security” is the delineation of the term as being highly general. Stewart and Jürjens (2018) expressed “Data Security” as a process including human factors. In contrast, we believe that the terminology for the construct is incorrect and as a result the notion of “security” within a FinTech perspective should be articulated under the term “Perceived cybersecurity”. The adjective “Perceived” refers to the fact that we do not seek to practically assess the cybersecurity of the FinTech mobile payments but rather grasp the consumer’s perception on cybersecurity. Cybersecurity is thus stemming from the discussion about commonalty and distinction between information security and cybersecurity (refer to section 2.2.1). We thus seek out to extend the notion of Cybersecurity by acknowledging the inputs of two socio psychological theories namely the Theory of Reasoned Action (TRA) and Extended Post Acceptance Model (EPAM).

Ryu (2018) developed a benefit risk framework by investigating what makes users willing or hesitant to use FinTech. In this perspective, Ryu (2018, p. 546) reflects upon the subject in a dual perspective, balancing the perceived benefits and perceived risks. Ryu (2018, p. 547), divided perceived risks into four dimensions including security risk.

Wang et al. (2003, p. 505) defined perceived risk and pointed out the complexity of objectively capturing risk due to its multidimensional nature. Nevertheless, we believe that in the context of FinTech it is possible to conceptually define within cybersecurity; the dimensions which may influence user’s acceptance. This thesis bases its preconception of perceived risk in terms of perceived security. We share the opinion of Lim et al (2018, p. 3), who conceptualized perceived security of FinTech as a multidimensional construct. The main argument for applying a multidimensional view on perceived security emanates from the fact that security is a mechanism which needs to be applied at numerous levels whether in the form of physical methods or application-based ones (Lim et al., 2018, p. 3; Gai et al., 2018, p. 264).
Lee (2015) stressed out the different layers including service security, platform security, network security and device security which are conceived as essential elements of the Internet of Things (which we have previously defined as the main domain of cybersecurity see section 2.2.2). Moreover, Hur and Lim (2017) extended the importance of perceived security to the IoT banking services. Subsequently if the importance is extensible to the IoT banking services we may also infer its application to FinTech mobile payment services. Perceived security may affect technological acceptance if understood as a cognitive process impacting both emotional and behavioral intention (Lim et al., 2018, p. 5).

In this line of argument, we assert that mobile FinTech services are linked to the former four layers of cybersecurity (i.e. platform, network, service, device) as permitting the ultimate use of the financial services (Hur & Lim, 2017). For instance, when users identify within the mobile FinTech service provided a higher level of security it inherently supports their expectation that the service extols stability (Hur & Lim, 2017).

The fact that the service exhibits security thus stability contributes to improve the usefulness of the service. It is precisely because of the “expectation” attribute depending on the presupposed security that the two constructs which are security and trust concur. Stewart & Jürjens (2018, p. 115) proposed within their research model the dimension “Customer Trust” thereby confirming that trust is a valuable aspect in the TAM model.

Despite the acknowledgement of the trust by different scholars (Luarn & Lin, 2005; Stewart & Jürjens, 2018), we believe that the ground foundation of trust used within these studies; does not fully reflect the online definition of trust. As we have formerly expressed, trust is a multidimensional concept which could be defined in different perspectives. Hur and Lim (2017) expressed that a higher level of security supports the customer’s expectation. Correspondingly, the customer’s expectation about the service corroborates the idea that within a FinTech context, trust will ultimately be perceived as the trustee’s ability to technically perform and respect its obligations towards the one included in the exchange (Barber, 1983). In other words, trust would be defined as trust in the technology which infers trust in its security. Nevertheless, solely defining trust in terms of trust in the technology does reduce trust to a single perspective which goes against its multidimensional nature. As we intend to investigate the FinTech phenomenon and more specifically the FinTech mobile payment segment, it is necessary to postulate our conceptualization of trust. The inputs of the personality theory, expectation risk theory, and institutional theory regarding the trust construct provide us the appropriate elements to define trust in the context of FinTech. Namely we articulate that the consideration of both trust as an expectation and trust as an institutional phenomenon convey the appropriate characteristics to converge with the online trust definition. Online trust has been defined from a psycho sociological perspective, characterized by a confident attitude towards an online situation of risk where one’s vulnerability will not be used (Corritore et al., 2003). The only distinction between offline and online is the context. The object of trust for offline trust is an individual however, for online trust the object is both the mean of exchange and the organization deploying the technology (Shankar et al., 2002). In other words, online trust is characterized by trust in the technology and trust in the organization providing the technology.
It is precisely because we delineate trust as converging to cybersecurity (trust in the security of the technology) and trust from an organizational point of view, that our conceptualization of trust within the TAM is novel and has been missing in the literature. Nonetheless, we still have to circumscribe how we define trust from an organizational perspective, to the extent trustworthiness of the company providing the technology. We believe that the best way to define trust in the organization is to therefore reflect on trust as perceived trustworthiness of the trustee. The online trust literature often exposes numerous dimensions which could be seen as trustworthiness attributes. Yet, we argue in the line of Lee and Turban (2001, p. 77) who articulated that trustworthiness comprises personal attributes useful for building trust. In essence, we intend to define trust in the organization as “reputation” and we seek out to solely select trustworthiness attributes that are converging to the concept of reputation. It is vital to select appropriate construct to support our delineation of online trust which would be applicable to the FinTech context.

As a result, the three trustworthiness attributes which have been selected are: Integrity, Ability and Benevolence (Mayer et al., 1995). Integrity is defined as the belief that the trustee agrees to a set of principles that the trustor found acceptable (Mayer et al., 1995). Ability thus refers to the fact that the trustee has the skills, characteristics or capabilities enabling them to have influence within certain domain (Mayer et al., 1995). Benevolence is interpreted as the trustee’s perception on the trustor that it wants to do well instead of maximizing profits (Mayer et al., 1995). These attributes have arguably been selected for three reasons. Firstly, they all convey the notion of perception from the trusting party perspective; to the extent they will be representing the consumer’s perceptions of the trusted party on certain attributes. Secondly, they are human like trust constructs (Lankton et al., 2015, p. 880) which therefore do not encroach the way we have defined trust in the technology. Lastly, all these attributes are mentioned to include the concept of reputation (Lee & Turban, 2001, p. 77).

In conclusion, after discussing and shedding the light on the deficiencies of the various theories addressing the technological acceptance; we have decided to further elaborate the research model of Stewart and Jürjens (2018). Their model originally comports five dimensions respectively Data Security (DS), Customer Trust (CT), Value Added (VA) including Perceived Usefulness (U) and Perceived Ease of Use (E), FinTech Promotion (FP), and User Design Interface (UI). Based on Stewart and Jürjens model about FinTech acceptance model (2018), we postulated a different conceptualization of both “Data Security” as “Perceived cybersecurity” (i.e. service security, platform security, network security and device security) and “Customer Trust” as trust in the technology therefore converging to “Perceived security” and trust in the organization (i.e. Organizational trust) which has been defined in terms of: reputation understood as ability, integrity and benevolence. We also did not take into consideration the FinTech Promotion (FP) variable as it was not motivated by any literature.
Our revised model of Stewart and Jürjens (2018) will be exposed hereinafter in Figure 4.

Figure 4. Conceptual model.

N.B. Perceived cybersecurity comprises service, platform, and device and network security. Organizational trust comprises integrity, benevolence, and competence.
4. Methodology

4.1 Choice of subject

We have selected our topic based on different reasons. Firstly, the phenomenon that is representing FinTech is novel in itself and its disruptive innovative feature makes it particularly interesting as we are both studying programs related to the field of Finance. As such, the impact of a new trend primarily promoted by the advent of the Information Communication Technology (ICT) and its repercussions onto the traditional finance and banking industry; are of interest. Along this line, we have both followed a course called “Current trends in Finance” and part of the course learning outcomes was to identify the ongoing trends which are affecting our respecting field of studies. Moreover, within the same course, we had the opportunity to attend to a presentation exposing the particular topic of FinTech but rather under the scope of RegTech. These different elements in combination with the recent application of the GDPR regulation motivated us to further investigate the FinTech phenomenon and its challenges in regard to the information security topic.

4.2 Research approach

There are different approaches when conducting a study. In essence, the choice of theoretical approach or research approach depends on the consideration of several elements: the first one is usually referred to the research paradigm, itself composed by the fundamental assumptions such as epistemology and ontology (Bryman & Bell, 2015, p 27). The fundamental assumptions are defining the philosophical stances that we as researches are considering about the theory of knowledge and the nature of social entities. In essence, to select the social research strategy we have to make sure that it is in line with the aim of the thesis conducted. In general, researchers must consider the nature of the relationship between theory and the social research and as such two broad categories emerged: deductive and inductive (Bryman & Bell, 2012, p. 24). The two theories are implying processes that are specific to them. Lastly, the research strategies are broadly categorized between quantitative and qualitative, which differs primarily based on their orientation to the role of theory in relation to research, and fundamental assumptions (Bryman & Bell, 2012, p. 36).

4.3 Fundamental assumption

4.3.1 Epistemological assumptions

Epistemology addresses the theory of knowledge and is broadly divided into two different categories; interpretivism and positivism (Bryman & Bell, 2012, p 53). However, the thesis adopts a critical realism approach, in believing that the variables which have been selected based on the literature are provisional and may evolve over time. The FinTech phenomenon corresponds to a broad taxonomy including many different applications: for instance, peer to peer, customer intimacy, payments, personal financial management, underbanked innovation, compliance (Freij, 2018, p. 35). The current study will concentrate on one of FinTech segment namely payment as it is the prominent segment right now.
Nevertheless, the variables which have been selected may be different in another domain, and or in another setting: due to the social and cultural or demographic perspectives. Consequently, the variables may not fully represent the consumers’ attitude towards technological acceptance within the entire FinTech industry. Critical realism is recommended as it allows us not only to use a hypothetical deductive approach but also give sense to the results by interpreting them in the name of realism (Bryman & Bell, 2012, p. 29). Moreover, as the current study will be based on self-questionnaire which thereby reasserts our willingness to not directly interfere in the respondent’s answers. The former thus creates objectivity which is in line with a critical realism stance.

4.3.2 Ontological assumptions

As expressed by Bryman and Bell (2012, p. 32), ontology deals with what is referred to as the nature of social entities. In essence, ontology raises the question whether social entities should be perceived as objective where reality is external from social actors, or if social entities are constructed and thereby deriving from the perceptions and action of social actors (Bryman & Bell, 2012, p. 32). The aim of the thesis is to determine whether “Perceived cybersecurity” and “Organizational trust” are part of the antecedents modelling customer’s technological acceptance of FinTech payment solutions.

Even though realism seems to be the most appropriate, we believe that that constructionism is the most relevant assumption as we intend to investigate firstly customer’s perceptions, and secondly constructs that are regarded as multifaceted (i.e. Perceived cybersecurity and Organizational trust). For instance, we have mentioned that the concept of Trust is a multidimensional construct and as such Trust is inherently constructionist as it implicitly questions how Trust is constructed. The existing literature on trust always mentions trust as a perception stemming from one party about another.

Additionally, trust is also individually constructed as everyone may have a different propensity to trust due to the different experiences they had. Lastly, the way we consider Trust in relation to our context (FinTech) forces us to regard trust from an online perspective. As such trust can be interpreted as: trust in the technology provided and trust in technology provider (organizational trust), thereby addressing a potential paradox between “image” and “identity”. In other words, one can be genuinely trustful, but trust can also be branded. Furthermore, the notion of trust will be proper to the context, time and culture under study; in our case Sweden.

4.4 Research strategy and design

As we have previously mentioned our thesis will aim to investigate the role of “Perceived cybersecurity” and “Organizational trust” in regard to the technological acceptance of FinTech payment solutions. The current thesis will consider the two dimensions as part of the Technological Acceptance Model (TAM) and will therefore consider a customer perspective by elucidating whether “Perceived cybersecurity” and “Organizational trust” amongst other selected variables; could be the antecedents of the customer’s technological acceptance of FinTech payment solutions.
In the present study a deductive approach is primarily adopted and motivated by the study aim. The choice of the deductive approach is also motivated by the process of the approach itself. In essence, we have revised the existing literature and combined in a different way by extending the model of Stewart and Jürjens (2018). As such, our intention is to postulate hypotheses that we will be testing by first collecting data throughout an online survey. After testing the model, we have extended we are interested in revising the theory originally generated. Additionally, since the study will be combining existing knowledge in a novel way, we framed a hypothetical deductive conceptual model thereby supporting our believes that the study of consumer behaviour and more specifically technological acceptance within FinTech can be fragmented and explained by a process (Bryman & Bell, 2012, p. 24). The nature of the research is exploratory-descriptive as the field is under expansion.

In the current study, we have chosen to conduct a quantitative research seeking to test from a customer perspective, the antecedents which may affect their technological acceptance of FinTech payment solutions.

The current study will be using a cross sectional design, where the collection of data will be done on more than a case at a single point of time (Bryman & Bell, 2012, p. 102). The main advantage of this approach is that it allows conducting a survey design which will help gathering data from numerous individuals at a single point of time, which in final will constitute a potential screenshot of customers and their perceptions about the antecedents affecting their technological acceptance of FinTech payment solutions. We also acknowledge the fact that it would have been better to conduct a longitudinal study as the FinTech phenomenon is gaining momentum and that the individuals which may already be using such solutions might only be representing Millennials. However, this type of study cannot be undertaken regarding time constraints.

4.5 Literature and source criticism

In order to conduct a thorough thesis, we initially made sure to rely on appropriate literature and theories. As a result, we have primarily decided to conduct our researches through Umeå's University library’s webpage, and we have also used Google Scholar. In order to be efficient in the way the researches were conducted, we took the time to identify the necessary dimensions impacting our topic such as: Information security, Data security, FinTech, Digitalization, Technological acceptance, online trust etc. Once the main themes were identified, we decided to look into the different keywords used by the articles, books and even reports. We decided that we should find relevant academic literature to support our topic and as such we have filtered our researches to the period 2015 to 2018 for the FinTech dimension. Even though the articles, books were recent, we always decided to search for the original articles or scholars mentioned to make sure that the interpretation of the so-called articles was in line with the original work. It also helped us to avoid indirect citations. All of the articles or books found were empirically grounded and peer reviewed in order to support quality and trustworthiness.
5. Methods & data

5.1 Sampling method

Sampling is broadly defined by two methods: probability sampling and non-probability sampling. The first one refers to a sample which has been chosen using a random selection permitting each unit of the population to be selected (Bryman & Bell, 2012, p. 187). The second one is the opposite of the probability sampling (there is no random selection). The present thesis will use a convenience sample method by using a list-based sampling frame. The main reasons motivating a convenience sample are the following: first, convenience sampling is chosen since it meets practical criteria such as accessibility, geographical proximity, and availability at a given time (Ilker et al., 2016, p. 2). The list-based sampling frame simply refers to the fact that a list of addresses will be used in order to communicate the internet-based survey. As mentioned by Fricker (2008, p. 2002) internet-based surveys can be conducted through web or email, however the invitation to take the survey is almost always done by email. As it is impossible to find an email list of all the consumers in Sweden, the survey approach will assemble a list-based sample of students at Umeå's University.

The first issue with using a convenience sample is the limitation it brings to the data collected. In our case, the convenience sampling is usually implying homogeneity of the population (Ilker et al., 2016, p. 2). Homogeneity would therefore be represented in our case by dimensions such as “culture”, “age” and “higher education”. In other words, the results will not be representative of the entire consumers in Sweden, as it may over represent one part of the population.

Nevertheless, heterogeneity may be emphasized in a list-based sample (e.g. students) by diversifying the educational background, considering each individual propensity to trust, and understanding of “culture” as socially and individually constructed.

Convenience sampling does not ensure representativeness of the population but is beneficial in the sense that it allows us to select participants which have access to online technologies, yet it does not ensure that they are using FinTech payment solutions. Furthermore, regarding the nature of the study convenience sampling is suiting the exploratory-descriptive perspective. The questionnaire will be administered in English which may affect the questionnaire’s understanding and response rate. As a result, a pilot test study will be conducted in order to reduce misunderstandings and ensure comprehension. Nevertheless, English proficiency will indeed represent a limitation. For the following reasons, the study acknowledges the fact that a convenience sample will not be representative of the entire consumers in Sweden, subsequently the results of such sample will lack of generalization.
5.2 Data Collection

5.2.1 Questionnaire

The questionnaire type for this thesis is a self-administered questionnaire where respondents answer the questionnaire without the intervention of the researchers. The questionnaire is available in Appendix 1. In this thesis, we have decided to conduct a web survey. The web survey will be distributed through emailing the selected respondents and invite them to visit a website at which the questionnaire will be available. We are using a web survey primarily because it will help gathering data that can directly be downloaded into a database while avoiding coding and typing errors (Bryman & Bell, 2012, p. 330). The literature review as well as the theoretical frame of reference was primordial to determine the selected variables. The variables have been inspired by the following authors:

Table 1. Variables and their origins.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Origins</th>
<th>Recent literature using the dimensions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived cybersecurity defined as: service, platform, network and device securities</td>
<td>Hur and Lim (2017)</td>
<td>Hur and Lim (2017)</td>
</tr>
<tr>
<td>Organizational trust defined as integrity, ability and benevolence</td>
<td>Mayer et al. (1995)</td>
<td>Shankar et al. (2002); Lankton et al. (2015).</td>
</tr>
</tbody>
</table>

Most of the questions have been adapted from existing questionnaires as the original questionnaires did not consider a FinTech perspective or were biased in the way the questions were stated. To send out the self-administered questionnaire, we firstly used emailing in order to redirect prospective respondents to the survey which was designed on google form. Within the survey, the author used a Likert scale ranging from 1 to 5. The Likert scale is primarily used so that the respondents may express their feelings regarding the selected statements (Bryman & Bell, 2012, p. 166). We have gathered 5000 email addresses from which 500 were not usable. We have decided to send a series of emailing of around 1000 emails a day for 5 days. We did not send a reminder to answer the survey as it was considered to be too invasive for the respondents. The data collection was made between 3rd March 2019 and 13th March 2019.
5.2.2 Pilot study

Beforehand to the distribution of the self-administrated questionnaire, we have decided to conduct a pilot study to ensure the following: First to ensure that the questions designed are not oriented thereby creating a bias in the answers. Secondly, in order to ensure clarity for the respondents. Thirdly to assess if the questionnaire contains questions that make respondents feel uncomfortable. Fourthly, we decided to gauge if the questionnaire is short and concise enough for respondents not to get lost at certain junctures. Lastly, we wanted to see if questions are often not answered and if there are any specific reasons for skipping the questions, for example confusing phrasing, poor instructions or unfitting positioning in the questionnaire (Bryman, 2012, p. 263). Finally, in order to correct any type of errors concerning the language. We conducted the pilot study in the form of interviews with different people where we asked the participants to independently do the questionnaire. After they did the questionnaire, we wanted to hear their general feedback but also their opinions on some specific questions and parts of the questionnaire. In total we asked five different people and we tried to make sure to ask people with different ages, nationalities and faculties that will also be asked later in the real study. Based on the pilot study, English speakers have advised to change the wordings and instructions, and most participants advised to change some scales for the questionnaire. Some feedback included that the questionnaire is confusion and unclear structured which is why we changed the structure and divided the questionnaire in different sections where respondents can only see one section at a time. This might also prevent respondents from thinking that the questionnaire is too long and increase their motivation to finish the questionnaire.

5.2.3 Social and Ethical perspectives

As we are conducting a self-administrated questionnaire, it is necessary to address how we considered the ethical perspective. In order to ensure an ethical behaviour, we have decided to consider four aspects which have been mentioned by Bryman and Bell (2012, p. 135):

1. No harm to participants.
2. No lack of informed consent.
3. No invasion of privacy
4. No deception.

Regarding the first element, we will send out an online questionnaire thereby we will not create any physical harm to the participants. The only issue with an online questionnaire is the fact that we will be contacting them without their permission through emailing.

According to the new GDPR regulation, we ensured that people receiving the emailing will not be able to see the other recipients. In order to achieve that matter, the emails were sent by using the Bcc option of Gmail. Bcc stands for blind copy carbon; therefore, the recipients cannot see the other contacts in the emailing. Nevertheless, as we are all part of the same educational Institution, we believe that the emails sent will be accepted and not considered as invading their privacy.
All the prospective respondents will be informed about the purpose of the study and will be given the choice to voluntarily fill in the questionnaire and be able to withdraw at any time (Saunders et al., 2012). Furthermore, as the questionnaire will include different demographics or opinions about statements, we will make sure that all answer given will remain anonymous and confidential. We will also ensure that the participants can only answer the survey once.

5.3 Data analysis

In this thesis, we will be using SPSS and STATA which allow quantitative data analysis (Bryman & Bell, 2011, p. 719). As we proceed to an online questionnaire through google form, the answers will be directly sent to a csv file which we will download into excel to proceed to transcription. The original data is usually “text” and not “numerical”. Therefore, we must recode the data. In order to avoid coding manually, we have used the IF formula of excel. We have used similar functions for the question on overall experience in terms of security and overall trust in the companies providing mobile payment applications.

In order to provide a general understanding regarding the data analysis, we have decided to describe, explain and motivate the different statistical tests which will be later on more detailed and conducted.

Our data analysis will be divided in three main sections:

- The first section is exposing a factor analysis and Cronbach’s Alpha.
- The second section is exposing the binary logistic regression.
- The third section is exposing the multiple regression.

The objective of the first section is to conduct a factor analysis. Factor analysis is a procedure commonly used and operates on the notion that variables may be reduced into a smaller set of variables that share common variance. In essence, factor analysis allows reducing dimensionality (Yong & Perce, 2013). Reducing dimensionality in our case is important, as each statement of a questionnaire creates a variable. Based on our questionnaire in Appendix 1, we can see that we have in total 31 statements and therefore we would get 31 variables.

The factor analysis will permit to reduce the number of variables by assessing whether they are related to a specific construct. In other words, instead of having each of the questions of our online survey as a variable, this particular test will help us to reduce the number of variables by checking whether the questions from our online survey are representing the same construct.

Once the constructs are created, we are using Cronbach’s Alpha as a measure of reliability. If the Cronbach’s Alpha is acceptable superior to 0.7 (Tavakol & Dennick, 2011, p. 53), then we can continue with other analyses. We will expose in Figure 5 the theoretical expectations and process of the factor analysis (see next page).
Depending on the factor analysis performed, we have the option to save the results as regression factors. The regression factors will therefore be the basis for the further analyses: such as multiple regression and binary logistic regression.

5.3.1 Descriptive statistics

All the data will be given in the Appendix 2. In the descriptive statistics section, the study will only expose the descriptive results about our data, namely exposing the results from the first two sections of our online survey.
5.3.2 Factor analysis & Cronbach’s Alpha

In this thesis, we will be conducting an exploratory factor analysis to decide on the factors to either include or exclude for our model. Once again, the aim of factor analysis is to reduce the number of variables. There are two types of factor analysis, namely confirmatory factor analysis (CFA) and exploratory factor analysis (EFA). An exploratory factor analysis is often conducted when one intends to discover the number of factors influencing the measured variables and their correlation (Yong & Pierce, 2013). In order to conduct an EFA there are several steps.

The first step is to take into consideration the correlation matrix where correlations of $r = 0.3$ or greater is required. Along this line, two tests need to be conducted to assess of the suitability of the data for factor analysis: namely the Kaiser Meyer Olkin test where its measure should be of 0.6 or above and the Barlett’s test of sphericity which should be significant at $p < 0.05$ (Pallant, 2010).

The second step addresses the extraction method and how it will be selected (Williams et al., 2010, p. 5). There are many extraction methods and the most common ones are principal component analysis (PCA) or principal axis factoring (PAF). In this thesis, we will be using a principal component analysis as we are interested in finding specifically the common variance amongst different variables (or in our case statements). As such, we assume that the communality of every variable is 1. In other words, by relying on this assumption we intentionally transpose our data into constituent linear components (Field, 2009, p. 637). This specific method is called a principal component analysis, and it is the method used to run the factor analysis.

The third step is pinpointing which criteria will determine the extraction. In essence, the aim of data extraction is to simplify the analysis by reducing the number of items so that they load on factors. Once again, there are multiple ways of performing such task for instance: Kaiser’s criteria (eigenvalues), scree plot test, parallel analysis etc. (Williams et al., 2010, p. 6). In this thesis, we have decided to combine both a scree plot test and Kaiser’s criteria. This choice is motivated to appropriately extract the correct number of constructs.

The fourth step addresses the selection of rotational method which aims to maximize item loadings. Two techniques are often used: orthogonal rotation or oblique rotation (i.e. direct oblimin). The selection of rotation method should be based on the one that provides the best fit and factorial suitability (Williams et al., 2010, p. 9). In this thesis, we will be performing an oblique rotation with the method direct oblimin as the literature suggests an interrelation between the concepts of security and trust and that specific method allows correlation amongst variables.

The last element which will be investigated is Cronbach’s Alpha. Cronbach’s Alpha is a measure of internal consistency (Tavakol & Dennick, 2011, p. 53). In other words, we will be testing for each construct whether the questions designed are related to each other. Cronbach’s Alpha will give a score ensuring validity. Generally, the acceptable values of alpha are ranging from 0.7 to 1. A low alpha score could be explained by either low number of questions for a construct, or poor interrelation between the items (questions) (Tavakol & Dennick, 2011, p. 53).
Cronbach’s Alpha will be tested on the constructs after running the factor analysis; as such the constructs should be composed of the different variable coded. It is the combination of the coded variables which will be tested for internal consistency. If the combination of coded variables produces a low Cronbach’s Alpha, we will be forced to revise the factor analysis.

5.3.3 Logistic regression analysis

We already mentioned that the first step of our data analysis was to allow us to reduce dimensionality by performing a factor analysis. The factor analysis is thus giving us the option to save the extracted variables under a new variable referred to factor score. In this thesis, we are interested investigating the customer’s intention to use of mobile payment applications. As a result, we first would like to know who from our respondents is carrying out payment transactions with a mobile payment application and which variables are likely to influence them. In other words, we first would like to investigate if Perceived Usefulness, Perceived Ease of Use, User Design Interface, Perceived cybersecurity and Organizational trust are affecting our respondent’s payment intention by using a mobile payment application. The payment intention of our respondents is based on the question 7 in our questionnaire (see Appendix 1). The question 7 of our questionnaire is a binary question, which means that respondents are only allowed to select either “Yes” or “No”. The question 7 asked:

Do you carry out payment transactions using a mobile payment application?

As the answer to our questions produces a binary outcome “Yes” or “No”, we need to use the appropriate technique to analyse it. Logistic regression describes a statistical technique that is used to analyse this type data. A logistic regression is similar to the multiple regression but with an outcome variable that is categorical (for instance “Yes” or “No”) and predictor variables that are continuous or categorical. The logistic regression will be based on the following: “Yes” is coded 1 and represents the usage. “No” is coded 0 and represents non usage. Using logistic regression, we can find out which variables affect the person’s usage of mobile payment application. Logistic regression also needs two assumptions to be met: Independence of errors and no multicollinearity problem.

The first is independence of errors which means that cases of data should not be related, because you cannot measure the same people at different points in time, but since we do a cross sectional study we do not need to check for this assumption because we only have one case of data (Field, 2009, p. 273).

The second assumption is about no multicollinearity problem which means that independent variables (i.e. Perceived Usefulness, Perceived Ease of Use, User Design Interface, Perceived cybersecurity and Organizational trust) should not be too highly correlated to each other. Multicollinearity in logistic regressions can be tested the same way as in multiple regressions, for example, through creating a Pearson correlation matrix among independent variables or to look at the Variance Inflation Factor (VIF) of the linear regressions (Field, 2009, p. 273).
5.3.4 Multiple regression analysis

Multiple regressions correspond to a statistical technique analysing data. It is referred to multiple regressions as it considering the relationship of multiple variables (i.e. independent variables) on a dependent variable which is also known as outcome (Leech et al., 2003, p. 738). In our case, the independent variables are: Perceived Usefulness, Perceived Ease of Use, User Design Interface, Perceived cybersecurity and Organizational trust. Furthermore, our dependent variable is customer’s intention to adopt FinTech. To conduct the multiple regressions properly, there are several assumptions that should be considered: normality, homoscedasticity, linearity, and no multicollinearity problem.

The normality assumption refers to the fact that for any specific value of any of the independent variables, the values of the dependent variable are normally distributed. The residuals should also be normally distributed. In order to check for normality one can either check visually using a histogram or QQ-plot or check the normality of residuals with the Shapiro Wilk test or Kolmogorov Smirnov test.

Furthermore, the variance for the normal distribution of possible values for the dependent variable must be the same as for each independent variable. This is called homoscedasticity.

Additionally, the independent variables must be related to the dependent variable in a linear way. This is called linearity assumption and is important because only linear relationships make contributions to the regression model (Richardson, 2015, p. 72). In order to detect linearity, we will be looking at the scatter plot of the dependent variable “intention to use” with each independent variable.

Another important assumption is no multicollinearity problem, meaning that the independent variables should not be too highly correlated with each other. If the independent variables are highly correlated with each other, it will create the problem of multicollinearity (Leech et al., 2003, p. 739). The first way of testing correlation would be to create a Pearson correlation matrix among independent variables. The second way is to look at the Variance Inflation Factor (VIF) of the linear regressions.
6. Empirical data and results

6.1 Sample procedure and characteristics

Due to the new GDPR regulation and its application, Umea University was not allowed to share a student electronic email list with us. As a result, we had to make a specific application to Ladok. The application gave us the right to obtain a physical paper form of the email list. In essence, we did not have a specific target besides ensuring that part of our respondents was actual users of FinTech mobile payment applications. In order to ensure diversity amongst our sample, we decided to select an even number of females and males in each faculty at Umea’s University. Umea’s University has four faculties: namely Faculty of Arts, Faculty of Medicine, Faculty of Social Sciences, and Faculty of Science and Technology. Out of original the 5000 emails collected, 4500 emails were sent between the 3rd March and the 13th March. The difference between the amount collected and the actual amount is explained by the fact that several of the email addresses were incorrect. It could also be explained by the fact that all email addresses had to be converted from a paper format to an electronic one. In order to convert the email list, we scanned the email list and then converted it to text by using Word 2016 function. The emails were then saved as a csv file so that it could be uploaded as a contact list into Gmail. Out of 4500 emails sent, 366 individuals took the online survey through the google form document. However, five responses were discarded since they were not complete. The response rate is 8.13 %. The response rate even though low is not alarming for this type of survey; the response rate usually fluctuates between 5 to 10%. The response rate is explained by the support used (i.e. emailing), the fact that no reminder was send and also by the target which is University students.

6.1.1 Demographics

In this section, we will be exposing the different demographics of our sample as well as some general information. The results correspond to the first section of our questionnaire. The demographics are based on the 361 answers which were valid. Based on 361 answers, our sample exhibits a predominance of females representing 60% in comparison to 40% males as exposed in Figure 6.

![Q1. Gender repartition](image)

Figure 6. Gender repartition.
The second question of our online questionnaire aimed to determine the age repartition of the respondents. The age categories were formed with a seven-year interval. The results are exposed in Figure 7.

![Figure 7. Age repartition.](image)

Based on Figure 7 and out of the 361 answers, 190 respondents were between 18-24, 135 were between 25-31, 26 were between 32-38, 6 were between 39-45 and 4 were 45+. Our sample is mostly represented by individuals between 18 to 31 years old (aggregating 90 % of the respondents). The last question regarding demographics allows us to categorize our respondents based on their educational background. The educational background is interpreted in terms of belonging to Umeå’s University faculties and is exposed in Figure 8.

![Figure 8. Faculty repartition](image)
Based on Figure 8, we can notice that majority of our respondents are from the Faculty of Social Sciences representing 40%, Faculty of Medicine represents 31%, Faculty of Science and Technology represents 20% and Faculty of Arts represents 9%.

6.2 Descriptive statistics

In this part, we will be presenting the results from the second section from our online questionnaire. The descriptive statistics are exposed in the Appendix 2. The section comports five questions. The first question (i.e. question 4 of our questionnaire), is gauging their awareness concerning the word “FinTech”. This question was intended in order to test whether the respondents knew the neologism and or the taxonomy that is FinTech. Out of 361 individuals, 300 were not aware of the word “FinTech” thereby representing 83.1% of our sample. Only 16.9% (61 individuals) confirmed their awareness of the word “FinTech”. The second question (i.e. question 5 of our questionnaire) was designed in order to assess three features: firstly assess the respondent’s usage of a mobile application related to a financial service, secondly evaluate whether the respondent’s usage could be related to a financial service but not related to a mobile payment service, and lastly cross compare their answers with their awareness of the neologism “FinTech”. The results are surprisingly interesting. To the question “Are you using a mobile application related to a financial service?” 314 individuals answered yes, 30 answered no and 17 were irresolute. If we compare these results with the awareness, we can notice that individuals are not aware of the word “FinTech” yet are mostly using a mobile application related to a financial service. For instance, 300 individuals were not aware, yet 314 individuals are using such service (and eventually 17 more). The 17 individuals which were irresolute could be explained by the understanding of what is a financial service.

The third question (i.e. question 6 of our questionnaire) was designed in order assess the respondent’s intention to use a mobile payment application. The results are exposed in the Figure 9.

![Figure 9. Intention to use mobile payment applications.](image-url)
The question 6 is crucial as it will be the question used in order to form the dependent variable in our multiple regression analyses. The scale used for this question was designed based on a Likert scale but modified in terms of labelling from very low to very strong. Out of 361 answers, 16 respondents considered their intention to use a mobile payment app as very low, 21 as low, 92 ranked their intention as occasional, 117 as strong and 115 as very strong. Based on this question, we notice that only 64.26 % are firmly decided to use a mobile payment application, 25.48 % would be categorized as occasional or contextual user and 10.26 % would not or rarely use it.

The fourth question (i.e. question 7 of our questionnaire), was designed to explicitly ask the respondents if they carry out payment transactions with a mobile app. The respondents had the choice to answer in a binary way by either saying yes or no. The question 7 will be used as dependent variable in our binary logistic regression. Out of 361 individuals, 331 answered yes and 30 answered no.

The fifth question was designed in order to get a classification of the respondents in terms of mobile payment service used. It is a multiple-choice question. We originally selected the potential answers by considering the geographic location as main argument. Therefore, the classification includes the following options: Swish, Klarna, Gpay, Apple pay, Paypal app, Alipay, Wechat pay, others and none. The results are exposed in the Figure 10.

---

**Q8. Which mobile payment service are you using?**

<table>
<thead>
<tr>
<th>Service</th>
<th>Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>50</td>
</tr>
<tr>
<td>Others</td>
<td>15</td>
</tr>
<tr>
<td>Wechat pay</td>
<td>10</td>
</tr>
<tr>
<td>Alipay</td>
<td>20</td>
</tr>
<tr>
<td>Paypal app</td>
<td>50</td>
</tr>
<tr>
<td>Samsung pay</td>
<td>10</td>
</tr>
<tr>
<td>Apple pay</td>
<td>10</td>
</tr>
<tr>
<td>Gpay</td>
<td>20</td>
</tr>
<tr>
<td>Klarna</td>
<td>150</td>
</tr>
<tr>
<td>Swish</td>
<td>150</td>
</tr>
</tbody>
</table>

---

**Figure 10.** Ranking of mobile payment services by usage.

As we expected, the fact that the study is conducted in Sweden has influenced the results since Swish and Klarna are two mobile payment services the most standing out. Out of 361 respondents, 324 are using Swish and 191 are using Klarna, 71 are using a different mobile payment service, and 53 are using Paypal app. (N.B: the respondents had the possibility to select several mobile payment services therefore the values do not aggregate to 361 in total).
6.3 Factor analysis: Principal component analysis.

The original questionnaire includes twenty broad questions from which eight are demographics and descriptive. The last twelve questions are assessing different dimensions. For instance, as we are interested to determine whether Perceived cybersecurity and Organizational trust influence the customer’s intention to use a FinTech mobile payment application; we have previously decided to further develop the Technological Acceptance Model (TAM) by considering the following elements: Perceived Usefulness, Perceived Ease of Use, User Design Interface, Perceived cybersecurity and Organizational trust. Each of the elements represent a dimension which itself include statements. Each statement represents a question where the respondents expressed their degree of approval based on a Likert scale (1 to 5).

- Perceived Usefulness comports four statements.
- Perceived Ease of Use comports three statements.
- User Design Interface comports three statements.
- Perceived cybersecurity comports four dimensions: i.e. service security, platform security, network security and device security. Service security has four statements, platform security three statements, network security has three statements and device security has three statements.
- Organizational trust comports three dimensions: i.e. integrity, benevolence, competence. Integrity has three statements; benevolence has three statements and competence two statements.

Factor analysis is a procedure commonly used and operates on the notion that variables may be reduced into a smaller set of variables that share common variance. In essence, factor analysis allows reducing dimensionality (Yong & Perce, 2013). Reducing dimensionality in our case is important, as each statement of a questionnaire creates a variable. We have in total 31 statements and therefore we would get 31 variables. Nevertheless, the factor analysis will permit to reduce the number of variables by assessing whether they are related to a specific construct. Theoretically we would want that all the statements regarding a specific dimension would relate to the same construct. For instance, all statements regarding Perceived Usefulness should relate to one construct that we would call Perceived Usefulness. Conducting a factor analysis will allow verifying if all statements are loading on the “correct” factor.

There are different types of factor analyses and they depend on our assumption about the data. As previously mentioned, when running a factor analysis, we are interested in finding specifically the common variance amongst different variables (or in our case statements). As such, we assume that the communality of every variable is 1. In other words, by relying on this assumption we intentionally transpose our data into constituent linear components (Field, 2009, p. 637).

This specific method is called a principal component analysis, and it is the method used to run the factor analysis. In this thesis, we have applied a cut off value of 0.4 for the factor loadings, implying that variables loading with a lower score will not appear in the results. We ran several factor analyses in order to make sure that all relevant items would load on a single factor.
The second step in the factor analysis is to consider the factor rotation: the factor rotation could either be orthogonal or oblique. We have considered an oblique rotation thereby allowing the factors to correlate. This choice is primarily motivated due to suggestions that the literature makes about the concept of Trust and Security as inducing interrelation.

The Table 2 below will expose the coding for each item. Each statement creates a variable coded in relation to its theoretical dimension.

Table 2. Factor analysis and variable coding.

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Number of Statements</th>
<th>Variable coding</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Usefulness</td>
<td>4</td>
<td>U1, U2, U3, U4</td>
</tr>
<tr>
<td>Perceived Ease of Use</td>
<td>3</td>
<td>E1, E2, E3</td>
</tr>
<tr>
<td>User Design Interface</td>
<td>3</td>
<td>D1, D2, D3</td>
</tr>
<tr>
<td>Perceived cybersecurity:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service security</td>
<td>4</td>
<td>AS1/AS2/AS3/AS4</td>
</tr>
<tr>
<td>Platform security</td>
<td>3</td>
<td>TS1/TS2/TS3</td>
</tr>
<tr>
<td>Network security</td>
<td>3</td>
<td>NS1/NS2/NS3</td>
</tr>
<tr>
<td>Device security</td>
<td>3</td>
<td>SmS1/SmS2/SmS3</td>
</tr>
<tr>
<td>Organizational trust:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrity</td>
<td>3</td>
<td>I1/I2/I3</td>
</tr>
<tr>
<td>Benevolence</td>
<td>3</td>
<td>Be1/Be2/Be3</td>
</tr>
<tr>
<td>Competence</td>
<td>2</td>
<td>C1/C2</td>
</tr>
</tbody>
</table>

From the first factor analysis, the following variables are not loading on a proper factor and did not exceed absolute cut off value of 0.4: NS1, NS2 and NS3. Therefore, we discarded the dimension Network security in the next factor analysis. Furthermore, E1 and U2 were loading on two dimensions; as a result, we decided to exclude them. Lastly, C1 and C2 did not load on any of the dimensions; therefore, they have been taken away.

The principal component analysis (PCA) also tests for Kaiser Meyer Olkin (KMO) measure of sampling adequacy and represents the ratio of the squared correlation between variables to the squared partial correlation between variables (Field, 2013, p. 647). In essence the KMO test helps in understanding the nature of the correlation pattern. The KMO only varies from 0 to 1. In other words, a value close to 1 supports the idea of aggregating the data into different factors that are reliable. The rule of thumb for the KMO test is to accept the factor analysis if the KMO is superior to 0.8 (Field, 2013, p. 647).
The second element given by the PCA is the Barlett’s Test of Sphericity which tests the null hypothesis that the correlation matrix resembles to an identity matrix. In this case, it would simply mean that we are testing the extent how our variables correlate with each other. If we are in the case of an identity matrix then it would mean that the correlation coefficients are zero, implying that our variables are independent.

In other words, if this test is not statistically different from 0 then it would mean our variables are unrelated and we cannot extract the common variance to form factors. We want the test to be statistically significant where our result would be lower than the set p value of 0.05. We ran a PCA with the direct oblimin rotation and we obtained the following table:

Table 3. KMO and Barlett's test.

| Kaiser-Meyer-Olkin Measure of Sampling Adequacy. | .894 |
| Bartlett’s Test of Sphericity | Approx. Chi-Square | 4113.810 |
| df | 276 |
| Sig. | .000 |

Test on the variables

As we can see, the KMO is 0.894 therefore supporting our intention to reduce the dimensionality of our variables. The Bartlett’s test of sphericity is statistically different from 0 therefore we can conclude that variables are correlated with each other and suitable for a factor analysis. We can now confirm that the data and variables are suitable for the factor analysis. The next element we are interested in is to specify how the extraction should be executed. The point of doing a factor analysis is to reduce dimensionality as previously mentioned, and in order to do so we have to consider how the factors will be extracted and under which criteria. The most common extraction method is based on the Kaiser’s criterion and it is advocating retaining factors that have an eigenvalue greater than 1.

The reason why we have considered the Kaiser’s criterion relies on two features; firstly, the sample size and secondly the average communality. As mentioned by Field (2013, p. 641), the Kaiser’s criterion is more appropriate when the sample size exceeds 250 and the average communality is over 0.6. In our case, we have a sample size of 361 and an average communality of 0.655 (i.e. 15.721/24). The communalities are listed in Table 4 on the next page.
Based on the PCA with direct oblimin rotation we obtained the scree plot shown in Figure 11. The scree plot is plotting on the y axis the eigenvalues for each component.

![Scree Plot](image)

**Figure 11. Eigenvalues scree plot.**

The scree plot is ambiguous it shows different inflexion points at component 4 and 6. As a result, we have decided to compare the scree plot with the total variance table, which provides the eigenvalues for each of the components and to which extent each component explains the variance in our data (note that not all the components are listed below as we have 24 components). The total variance is exposed in Table 5 (see next page).

<table>
<thead>
<tr>
<th>Statements</th>
<th>Initial</th>
<th>Extraction</th>
<th>Statements</th>
<th>Initial</th>
<th>Extraction</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1</td>
<td>1,000</td>
<td>.667</td>
<td>TS1 value</td>
<td>1,000</td>
<td>.723</td>
</tr>
<tr>
<td>U3</td>
<td>1,000</td>
<td>.571</td>
<td>TS2 value</td>
<td>1,000</td>
<td>.758</td>
</tr>
<tr>
<td>U4</td>
<td>1,000</td>
<td>.551</td>
<td>TS3 value</td>
<td>1,000</td>
<td>.723</td>
</tr>
<tr>
<td>E2</td>
<td>1,000</td>
<td>.519</td>
<td>SmS1</td>
<td>1,000</td>
<td>.605</td>
</tr>
<tr>
<td>E3</td>
<td>1,000</td>
<td>.657</td>
<td>SmS2</td>
<td>1,000</td>
<td>.729</td>
</tr>
<tr>
<td>D1</td>
<td>1,000</td>
<td>.809</td>
<td>I1</td>
<td>1,000</td>
<td>.563</td>
</tr>
<tr>
<td>D2</td>
<td>1,000</td>
<td>.831</td>
<td>I2</td>
<td>1,000</td>
<td>.656</td>
</tr>
<tr>
<td>D3</td>
<td>1,000</td>
<td>.809</td>
<td>I3</td>
<td>1,000</td>
<td>.631</td>
</tr>
<tr>
<td>AS1</td>
<td>1,000</td>
<td>.710</td>
<td>Be1</td>
<td>1,000</td>
<td>.567</td>
</tr>
<tr>
<td>AS2</td>
<td>1,000</td>
<td>.743</td>
<td>Be2</td>
<td>1,000</td>
<td>.503</td>
</tr>
<tr>
<td>AS3</td>
<td>1,000</td>
<td>.630</td>
<td>Be3</td>
<td>1,000</td>
<td>.525</td>
</tr>
<tr>
<td>AS4</td>
<td>1,000</td>
<td>.543</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Table 5. Total variance explained.

<table>
<thead>
<tr>
<th>Component</th>
<th>Initial Eigenvalues</th>
<th>Extraction Sums of Squared Loadings</th>
<th>Rotation Sums of Squared Loadingsa</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Total</td>
<td>% of Variance</td>
<td>Cumulative %</td>
</tr>
<tr>
<td>1</td>
<td>7.674</td>
<td>31.977</td>
<td>31.977</td>
</tr>
<tr>
<td>2</td>
<td>2.847</td>
<td>11.861</td>
<td>43.838</td>
</tr>
<tr>
<td>3</td>
<td>1.683</td>
<td>7.014</td>
<td>50.852</td>
</tr>
<tr>
<td>4</td>
<td>1.250</td>
<td>5.207</td>
<td>56.059</td>
</tr>
<tr>
<td>5</td>
<td>1.198</td>
<td>4.992</td>
<td>61.051</td>
</tr>
<tr>
<td>6</td>
<td>1.068</td>
<td>4.450</td>
<td>65.502</td>
</tr>
<tr>
<td>7</td>
<td>0.915</td>
<td>3.812</td>
<td>69.314</td>
</tr>
<tr>
<td>8</td>
<td>0.826</td>
<td>3.442</td>
<td>72.755</td>
</tr>
</tbody>
</table>

a When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Based on Table 5, we can now be sure that we will retain the components from 1 to 6 as they all have an eigenvalues superior to 1. Moreover, the total variance table is interesting to interpret, as the first component with an eigenvalue of 7.674 is responsible for 31.977% of the total variance. The component 2 is explaining 11.861% of the total variance, the component 3 explains 7.014%, the component 4 explains 5.207%, the component 5 explains 4.992% and the component 6 explains 4.45% of the total variance. The six components extracted based on the Kaiser’s criterion explains 65,502% of the total variance.

As we have allowed correlation amongst components the percentage of the total variance after rotation cannot be produced. In other words, we are not able to know whether there is a change before and after extraction, and what is the effect of the rotation onto the total variance explanation.

Furthermore, we looked at the component correlation matrix in order to statistically confirm whether our motivation to use an oblique rotation is founded. If the component correlation matrix does not exhibit correlation between the factors, we can then conclude that is it an identity matrix and that an orthogonal rotation is more suited. However, the component correlation matrix is showing correlation amongst our factors. Finally, the pattern matrix exposes in Table 6, which variables are loading onto which component based on the extraction method and rotation (extraction based on eigenvalue and the rotation used is direct oblimin).
Based on the Table 6, we are now able to understand which components have been extracted and which variables are loading on the components. There are 6 components which were extracted and rotated, with the pattern matrix we are able to identify the components and name them. For instance, as all the variables AS1/AS2/AS3/AS4 loads onto the first component it suggests that the component 1 is service security. Following the same logic, the component 2 comprises variables from both User Design Interface and Perceived Ease of Use. As a result, it should suggest that design and ease of use are interrelated and could be clustered into one dimension that we labelled usability and ergonomics. The component 3 clusters the variables from Integrity and benevolence and represents Organizational trust. The component 4 aggregates the variables SmS1/SmS2/SmS3 and therefore suggests the device security. The component 5 clusters U1/U3/U4 and represents Perceived Usefulness. Lastly, the component 6 comprises TS1/TS2/TS3 and represents the platform security. The first conclusion which can be drawn is that not all the dimensions that we expected to test will be; as the factor analysis revealed the irrelevancy of one of the sub dimensions of Perceived cybersecurity (i.e. network security) and one dimension of Organizational trust (i.e. competency).
6.4 Cronbach’s Alpha

The principal component analysis conducted on 24 items with an oblique rotation (direct oblimin) produced a KMO of 0.894 and a significant Barlett’s test of sphericity Chi Square (df= 276) = 4113.810, p <0.001. The PCA extracted 6 components which had eigenvalues over the Kaiser’s criterion and that explained 65.502 % of the variance. In order to confirm the principal component analysis, it is necessary to verify whether the components extracted are reliable. As a result, a reliability analysis was conducted on each of the components extracted. The table below will expose the results of the reliability analysis by exposing the Cronbach’s Alpha.

Table 7. Reliability analysis.

<table>
<thead>
<tr>
<th>Original dimensions</th>
<th>Labels after PCA</th>
<th>Items contained</th>
<th>Cronbach’s Alpha</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived cybersecurity</td>
<td>Service security</td>
<td>AS1/AS2/AS3/AS4</td>
<td>0.798</td>
</tr>
<tr>
<td>Perceived Ease of Use and User Design Interface</td>
<td>Usability &amp; ergonomics</td>
<td>D1/D2/D3 E2/E3</td>
<td>0.876</td>
</tr>
<tr>
<td>Organizational trust</td>
<td>Organizational trust</td>
<td>I1/I2/I3 Be1/Be2/Be3</td>
<td>0.803</td>
</tr>
<tr>
<td>Perceived cybersecurity</td>
<td>Device security</td>
<td>SmS1 SmS2 SmS3</td>
<td>0.731</td>
</tr>
<tr>
<td>Perceived Usefulness</td>
<td>Perceived Usefulness</td>
<td>U1/U3/U4</td>
<td>0.712</td>
</tr>
<tr>
<td>Perceived cybersecurity</td>
<td>Platform security</td>
<td>TS1/TS2/TS3</td>
<td>0.800</td>
</tr>
</tbody>
</table>

As exposed in the Table 7, all the components from the PCA produced a Cronbach’s Alpha superior to 0.7 therefore confirming the reliability of the components and its items as ensuring consistency of the measure. The Cronbach’s Alpha for dimensions will be exposed in the Appendix 3 which contains the Cronbach’s Alpha if each of the item is deleted. We can now conclude that the components extracted from PCA are valid and reliable.

6.5 Factor scores

When conducting a factor analysis and in our case a principal component analysis, we have the option to save the factor scores as a new variable. There are several methods for calculating factor scores: respectively Regression, Anderson Rubin and the Barlett scores. As we have conducted a PCA with an oblique rotation thereby allowing correlation amongst variables we have decided to save the factor scores under the Regression method.

Under this method, the computed factor scores are standardized to a mean of 0 and if principal component method is used the standard deviation of the distribution factor scores will be 1 (Distefano et al., 2009, p. 4). The factor scores are now representing the component scores.
For instance, factor 1 corresponds to component 1 and the same logic applies to the other factors. As we had six components extracted from the PCA, we now have six regression factors. These factors representing each of the components will be used as independent variables when conducting the multiple regression analyses and the binary logistic regression. The Table 8 will expose now the different factors and their interpretations.

Table 8. Factor scores and interpretations.

<table>
<thead>
<tr>
<th>Factor score generated</th>
<th>Component correspondence</th>
<th>Factor score interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>FAC1_1</td>
<td>Component 1</td>
<td>Service security</td>
</tr>
<tr>
<td>FAC2_1</td>
<td>Component 2</td>
<td>Usability &amp; ergonomics</td>
</tr>
<tr>
<td>FAC3_1</td>
<td>Component 3</td>
<td>Organizational trust</td>
</tr>
<tr>
<td>FAC4_1</td>
<td>Component 4</td>
<td>Device security</td>
</tr>
<tr>
<td>FAC5_1</td>
<td>Component 5</td>
<td>Perceived Usefulness</td>
</tr>
<tr>
<td>FAC6_1</td>
<td>Component 6</td>
<td>Platform security</td>
</tr>
</tbody>
</table>

6.6 Binary logistic regression

In this section, we will be performing a binary logistic regression with STATA. Our dependent variable will be question 7 from our questionnaire: “Do you carry out payment transactions with a mobile application?” The respondents were asked to reply by “Yes” or “No”, therefore the dependent variable is considered as dichotomous. Our logistic regression produced a Wald Chi2 = 31.04 that is statistically significant Prob>Chi2 = 0.000, therefore suggesting a good fit between our model and the data. Furthermore, The Pseudo R squared is equal to 0.1875. The Table 9 will expose the robust logistic regression based on our model where Payment intention is our dependent variable (N.B: the coefficients are limited to three decimals and rounded).

Table 9. Robust binary logistic regression.

| Payment Intention | Coefficients | Robust Std. Err. | z     | P > |z| |
|-------------------|--------------|------------------|-------|-----|----|
| Service security  | -0.091       | 0.2422           | -0.37 | 0.709 |
| Usability & ergonomics | 0.391       | 0.3221           | 1.21  | 0.225 |
| Organizational trust | 0.059       | 0.2047           | 0.29  | 0.772 |
| Device security   | **0.491**    | 0.2131           | 2.30  | **0.021** |
| Perceived Usefulness | **0.702**   | 0.2275           | 3.08  | **0.002** |
| Platform security | -0.036       | 0.2467           | -0.15 | 0.884 |
| Constant          | 2.926        | 0.2222           | 13.17 | 0.000 |
We are trying to predict the payment intention of someone who answered yes by using our factors as predictors.

The results of the binary logistic regression show that:

- Service security has not been found to be statistically significant as $P>|z| = 0.709$.
- Usability & ergonomics has not been found to be statistically significant as $P>|z| = 0.225$.
- Organizational trust has not been found to be statistically significant as $P>|z| = 0.772$.
- Device security has been found to be statistically significant as $P>|z| = 0.021$, which is lower than the set p value of 0.05.
- Perceived Usefulness has been found to be statistically significant as $P>|z| = 0.002$, which is lower than the set p value of 0.05.
- Platform security has not been found to be statistically significant as $P>|z| = 0.884$.

Based on the results of the robust binary logistic regression, we can derive the following equation:

$$
Payment\ Intention = 2.926 + 0.491\ (Device\ security) + 0.702\ (Perceived\ Usefulness) + \epsilon
$$

Epsilon is a random error.

### 6.7 Multiple regression: factor scores and intention to use

In this section, we will be performing the multiple regression analyses with STATA. Originally, we expected the dependent variable to be “Customer’s Intention to use” and the independent variables would have been: Perceived cybersecurity, Perceived Usefulness, Perceived Ease of Use and Organizational trust. Based on the principal component analysis, we had to discard network security (as part of Perceived cybersecurity) and competency (as part of Organizational trust). As such, the dependent variable which we intend to predict is still based on question 6 from our questionnaire. Question 6 corresponds to the variable “Intention to use” of mobile payment applications. Nevertheless, the predictors in the multiple linear regressions are now the factor scores generated from our principal component analysis with an oblique rotation. In other words, we intend to predict “Intention to use” based on service security, usability & ergonomics, Organizational trust, device security, Perceived Usefulness and platform security.
Intention to use

\[ = \text{constant} + \beta_1 (\text{Service security}) + \beta_2 (\text{Usability & ergonomics}) + \beta_3 (\text{Organizational trust}) + \beta_4 (\text{Device security}) + \beta_5 (\text{Perceived Usefulness}) + \beta_6 (\text{Platform security}) + \epsilon \]

Where \( \beta \)'s are the different coefficients for each independent variable. Epsilon is a random error.

As we have previously mentioned in section 5.3.4 (i.e. about multiple regression), there are a variety of assumptions that needs to be tested before running the statistical procedure. The linearity assumption is assuming a linear relationship between the independent variables and the variable one. In order to test for this peculiar assumption, it is common to produce a scree plot of each independent variable with the dependent one. The visual inspection usually permits to identify linearity. In our case, the scree plots for each of the independents and dependent variable did not reveal any anomalies which would induce nonlinearity. Furthermore, the existing literature on the different concepts did not suggest evidences about nonlinearity, as such the linearity assumption is assumed.

Normality is usually defined in terms of normality about residuals. It is common to produce a histogram with a normal bell curve or plot a PP plot (i.e. probability of observed cumulated versus expected cumulated probability of regression standardized residuals. In our case, the PP plot revealed a deviation from normality (see Appendix 4), plus our data is skewed to the left. Normality is not met but not essential in our situation as we are assessing perceptions about individuals. As our data is none normally distributed, we must be sure to select the appropriate test for homoscedasticity. The two important assumptions that we should meet is no multicollinearity problem and homoscedasticity. The multicollinearity is tested by producing two outputs: first the Pearson correlation and secondly the Variance inflation Factor (VIF). Based on the Pearson correlation of all the independent variable and the dependent variable exposed in Table 10, we did not notice any correlation where \( r > 0.6 \).

Table 10. Pearson correlation for our conceptual model

<table>
<thead>
<tr>
<th></th>
<th>Intention to use</th>
<th>Service security</th>
<th>Usability &amp; ergonomics</th>
<th>Organizational trust</th>
<th>Device security</th>
<th>Perceived Usefulness</th>
<th>Platform security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intention to use</td>
<td>1.0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Service security</td>
<td>0.2485</td>
<td>1.0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Usability &amp; ergonomics</td>
<td>0.3581</td>
<td>0.2558</td>
<td>1.0000</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Organizational trust</td>
<td>0.3149</td>
<td>0.3027</td>
<td>0.1731</td>
<td>1.0000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Device security</td>
<td>0.2575</td>
<td>0.3285</td>
<td>0.2323</td>
<td>0.2551</td>
<td>1.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perceived Usefulness</td>
<td>0.4645</td>
<td>0.1590</td>
<td>0.3409</td>
<td>0.1447</td>
<td>0.1134</td>
<td>1.0000</td>
<td></td>
</tr>
<tr>
<td>Platform security</td>
<td>0.1912</td>
<td>0.3430</td>
<td>0.1643</td>
<td>0.2217</td>
<td>0.2953</td>
<td>0.1360</td>
<td>1.0000</td>
</tr>
</tbody>
</table>
The last assumption that needs to be tested is the homoscedasticity. As our data is not normally distributed, we have decided to conduct a White Test for heteroscedasticity. Under the null hypothesis, the White test suggests that the variances of errors are equal. The alternative hypothesis suggests that the variances of the errors are not equal. In order to test for that particular procedure, we first need to run the regression without testing for homoscedasticity. The first multiple regression of our model is included in the Appendix 5.

Based on the White Test results we obtained a Chi squared of 55.25 and we can reject the null hypothesis of homoscedasticity as the Prob > chi2 = 0.0011 is lower than the set p value of 0.05. Consequently, we accept the alternate hypothesis that there is heteroscedasticity amongst the residuals. As a result, we cannot trust the standard errors, the t values and the p values that have been produced in the first multiple regression analysis exposed in Appendix 5. In this particular case, we have the possibility to run a multiple regression under a robust method in order to counter the heteroscedasticity of our residuals. The second multiple regression has been to set to be robust in order to correct the standard errors, their t values and p values. The robust multiple regression on our model produced the F test and suggested that the regression model is a good fit for the data as F (6, 354) = 31.39, p<0.05. Furthermore, our model with a R-squared= 0.3283 explains 32.83% of the variability in our dependent variable. In other words, our model (i.e. the independent variables) explains 32.83 % of the variability of the “intention to use”. The Table 11 will expose the results of the robust multiple regression based on our conceptual model.

Table 11. Robust multiple regression on our conceptual model.

| Intention to use | Coefficients | Robust Std. Err. | t | P < |t| |
|------------------|--------------|------------------|---|-----|
| Service security | 0.053        | 0.058            | 0.92 | 0.359 |
| Usability & ergonomics | **0.175**    | 0.073            | 2.39 | **0.017** |
| Organizational trust | **0.202**    | 0.053            | 3.74 | **0.000** |
| Device security | **0.116**    | 0.054            | 2.14 | **0.033** |
| Perceived Usefulness | **0.388**    | 0.051            | 7.52 | **0.000** |
| Platform security | 0.028        | 0.050            | 0.55 | 0.583 |
| Constant         | 3.811        | 0.047            | 81.01 | **0.000** |

Based on the Table 11, we can notice the following:

- Service security has not been found to be statistically significant as the P>|t|= 0.359.
- Usability & ergonomics has been found to be statistically significant as the P>|t|= 0.017.
- Organizational trust has been found to be statistically significant as the $P>|t|=0.000$.
- Device security has been found to be statistically significant as the $P>|t|=0.033$.
- Perceived Usefulness has been found to be statistically significant as the $P>|t|=0.000$.
- Platform security has not been found to be statistically significant as the $P>|t|=0.583$.

As a result, after running the robust multiple regression we can derive our original equation to the following equation:

\[
\text{Intention to use} = 3.811 + 0.175 (\text{Usability & ergonomics}) + 0.202 (\text{Organizational trust}) + 0.116 (\text{Device security}) + 0.388 (\text{Perceived Usefulness}) + \epsilon
\]

Epsilon is a random error.

### 6.8 Multiple regression with overall security and trust as predictors

The last regression which has been conducted is based on two questions which have been asked to the respondents. The first question is part of the section 5 of our questionnaire and was designed to assess the overall experience of using mobile payment app in terms of security. For this question the respondents were informed what the following elements of security were to be considered and if one would be failing that security will be at stake. The second question is part of the section 6 of our questionnaire, and it was asking respondents to rate their overall trust regarding mobile payment application providers (the companies). The Overall security and trust will represent the independent variables, while the dependent one is still question 6 from our questionnaire (Intention to use). As the variables overall security and trust are slightly different than Perceived cybersecurity and Organizational trust since they are emphasizing both the respondent’s overall experience in terms of security and their overall trust in the companies providing mobile payment applications; we decided not to include control variables as in our regression about our conceptual model. In order to run the regression, we will be checking for the multicollinearity assumption and the homoscedasticity assumption. The tests are similar to the one previously done in section 6.7. The Pearson correlation exposed in Table 12 did not induce any multicollinearity problem.

<table>
<thead>
<tr>
<th></th>
<th>Intention to use</th>
<th>Overall security</th>
<th>Overall trust</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intention to use</td>
<td>1.0000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall security</td>
<td>0.2972</td>
<td>1.0000</td>
<td></td>
</tr>
<tr>
<td>Overall trust</td>
<td>0.3428</td>
<td>0.4020</td>
<td>1.0000</td>
</tr>
</tbody>
</table>
We first ran the regression without testing for homoscedasticity (see Appendix 6). Then, we have tested for homoscedasticity with the White Test we obtained a Chi2 (5) = 27.46 and we can reject the null hypothesis of homoscedasticity as the Prob > chi2 = 0.0000 is lower than the set p value of 0.05. Our data appears to have heteroscedasticity. As a result, we cannot trust the results from the first regression.

Due to the results of the White test, we have conducted the multiple regression analysis under the robust method. Once again, this method is correcting the standard errors and the t values and p values. The results of the robust regression are exposed in Table 13.

The robust multiple regression on our model produced the F test and suggested that the regression model is a good fit for the data as F (2, 358) = 30.01, and statistically significant as the Prob > F = 0.0000 which is lower than the set p value of <0.05. Furthermore, our model with a R-squared= 0.1478 explains 14.78 % of the variability in our dependent variable. In other words, our model (i.e. the independent variables) explains 14.78 % of the variability of the “intention to use”.

Table 13. Robust multiple regression with overall security and trust.

| Intention to use | Coefficients | Robust Std. Err. | t    | P > |t| |
|-----------------|--------------|-----------------|------|-----|---|
| Overall security | 0.258        | 0.091           | 2.82 | 0.005 |
| Overall trust   | 0.334        | 0.078           | 4.30 | 0.000 |
| Constant        | 1.684        | 0.307           | 5.48 | 0.000 |

Based on the Table 13, we can formulate the following:

- Overall security has been found to be statistically significant with a P>|t| = 0.005, which is lower than the set p value of 0.05.
- Overall Trust has been found to be statistically significant with a P>|t| = 0.000, which is lower than the set p value of 0.05.

We can also derive the following equation:

\[
Intention \ to \ use = 1.684 + 0.258 \ (Overall \ Security) + 0.334 \ (Overall \ Trust) + \varepsilon
\]

Epsilon is a random error.
6.9 Summary of the conceptual model

In this section, we will expose the final conceptual model based on the different tests run. First, we will present in Table 14 a comparison of the dimensions which we intended to test and the dimensions which have been tested.

Table 14. Comparison of the theoretical model and revised model based on PCA.

<table>
<thead>
<tr>
<th>Original model</th>
<th>Revised model after PCA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived Usefulness</td>
<td>Perceived Usefulness</td>
</tr>
<tr>
<td>Perceived Ease of Use</td>
<td>Usability &amp; ergonomics</td>
</tr>
<tr>
<td>User Design Interface</td>
<td></td>
</tr>
<tr>
<td>Perceived cybersecurity:</td>
<td>Perceived cybersecurity:</td>
</tr>
<tr>
<td>• Service security</td>
<td>• Service security</td>
</tr>
<tr>
<td>• Platform security</td>
<td>• Device security</td>
</tr>
<tr>
<td>• Device security</td>
<td>• Platform security</td>
</tr>
<tr>
<td>• Network security</td>
<td></td>
</tr>
<tr>
<td>Perceived cybersecurity:</td>
<td>Perceived cybersecurity:</td>
</tr>
<tr>
<td>Organizational trust:</td>
<td>Organizational trust:</td>
</tr>
<tr>
<td>• Integrity</td>
<td>• Integrity &amp; Benevolence</td>
</tr>
<tr>
<td>• Benevolence</td>
<td></td>
</tr>
<tr>
<td>• Competency</td>
<td></td>
</tr>
</tbody>
</table>

The Figure 12 will expose the revised model and the statistical significances based on the multiple regression.

![Revised conceptual model](image)

Figure 12. Revised conceptual model

N.B The green colour symbolizes statistical significance. The sign + suggests a positive relationship to Intention to use.
7. Analysis

7.1 Discussion related to the Factor analysis

As part of our statistical procedure, we have decided to run a principal component analysis. The aim of the principal component analysis is to reduce dimensionality by creating and extracting factors that best fit our data. Prior to the PCA, we had diverse expectations regarding the PCA and how the statements would load on each factor. For instance, we originally aimed to investigate Perceived Usefulness, Perceived Ease of Use, User interface design, Perceived cybersecurity, and Organizational trust. As such, we were expecting all of these dimensions to produce an equal number of factors.

Yet, the results of the PCA confirmed two features: first, that the variables were correlated with each other, and as such that the oblique rotation was the most appropriate. Now, we should take some time to elaborate on why correlation amongst our variables is important. In our case, the variables are interrelating. We have previously mentioned that we firmly believe that two dimensions were of high importance in the context of FinTech, and especially regarding technological acceptance. These two dimensions are information security and trust. We firstly argued for their multidimensionality but also for their role as antecedents regarding technological acceptance. It is precisely the contextualization of our study, namely the study of mobile payment applications and its link to the online trust literature that supported our theoretical ground. To some extent, we can conclude that the PCA converged with our pre-conceptualizations. Namely, the PCA emphasized the following: Perceived Ease of Use and User Design Interface loaded on the same factor.

We had thereby concluded that in the context of mobile payment applications (i.e. FinTech), the ease attribute and the design attribute are converging into a dimension that we have called; usability & ergonomics. This finding concurs with the fact drawn out by Stewart & Jürjens (2018, p. 115); who mentioned that security and trust should be studied in relation to usability. Additionally, the PCA suggested that only two of the dimensions of Organizational trust were relevant: integrity and benevolence. Competence has thus been discarded. Competence could have been discarded based on two facts: either as not being an appropriate dimension applicable to the study of intention to use, or because competence was already captured by another dimension. We suggest, the second alternative as the most likely since the mean of use (the fact that we are in an online environment) might reinforce antecedents such as usefulness and usability. For instance, Egger (2002) also stressed that usability is one of the vital factors of trust models in the context of interfaces.

Lastly, we were surprised to see that each dimension of the Perceived cybersecurity was actually loading on a different factor (N.B. The network security has been discarded). This result could be explained by the wide understanding of security especially when it comes to mobile payment applications. Security covers such a large spectrum in relation to cybersecurity and the Internet of Things (IoT), that each of the dimensions even though theoretically placed under the same label, may be in practical highly different and too specific to be directly linked to one concept.
7.2 Discussion related to the binary logistic regression.

In order to investigate Perceived cybersecurity and Organizational trust in the context of technological acceptance, we have first decided to run a binary logistic regression. The binary logistic regression is based on our question 7 in our online survey, where respondents were asked: Do you carry out payment transactions with a mobile app?

The respondents only had the option to select Yes or No. As such, the question indicates the number of users (i.e. customers) and the non-user or potential user. We emphasize the non-user or potential user perspective as a no does not necessarily mean they are not using a mobile payment application. In fact, it appeared that many of the respondents who answered “No” to the question 7 have then selected in question 8 a type of mobile payment thereby indicating that they are using a mobile payment app. In this sense, we want to underline that a no can be a false positive or a false negative, thereby stressing out the difference between users, unaware users, and non-users. It is a distinction that we need to consider when drawing our inferences and interpretations.

In our case, the binary logistic regression helps us to predict whether someone answered “Yes” and is thus categorized as user of mobile payment application and to the extent FinTech payment apps. The binary logistic regression allows us to have a first insight into intention use by considering the actual usage. The logistic regression was run with the factors from the PCA as independent variables under a robust method. The results are the following: Service security has not been found to be statistically significant, Usability & ergonomics has not been found to be statistically significant, Organizational trust has not been found to be statistically significant, Device security has been found to be statistically significant, Perceived Usefulness has been found to be statistically and Platform security has not been found to be statistically significant.

Out of the six factors from the PCA only two had been found to be statistically significant and their coefficients suggest a positive relationship. Device security and Perceived Usefulness have been found to be positive related to the actual usage of a mobile payment app. Device security has been defined the following way (see Appendix 1 section called smartphone security):

- Do you think your mobile is secure?
- Do you think your mobile is sufficiently performing to support the use of the mobile payment services?
- Do you think, your mobile was supplied by a trusted/certified salesperson?

Device security has comprised three perspectives; security through security methods, security through performance, and security through certification. In the same way, Perceived Usefulness which has been found significant was defined with the three following statements:

- Do you think mobile payment apps are convenient?
- Do you think mobile payment apps are fast?
- Do you think mobile payment apps are available as a payment method?

Perceived Usefulness was emphasizing convenience, responsiveness and availability.
In conclusion, firstly the test suggests Perceived Usefulness and device security are positively affecting our respondent’s usage. The respondents from our sample are mostly representing a user perspective (if we compare the proportion of positive including false positive with non-user), consequently we could extend by saying that Perceived Usefulness and device security are the primary factors that push users to carry out payment transactions with a mobile app. It appears that usefulness which comprises convenience, responsiveness and availability features can solely justify the usage of mobile payment applications. The fact that device security was also found significant is interesting. In other words, users who consider their phones secure did not necessarily see more risks in using a mobile payment app and are more likely to carry out the payment transactions based on its beneficial attributes. Along this line Ryu (2018) investigated what makes users willing or hesitant to use FinTech. In his model which was centred on the Theory of Reasoned Action (TRA), Ryu (2018) developed a benefits risk framework which was composed on the benefits perspectives by: economic benefit, seamless transaction and convenience. Ryu (2018) found that the three were statistically significant and positive with continuance to use FinTech. To some extent, our results converges with the ones of Ryu (2018, p. 560) where he concluded that in general perceived benefits have a stronger impact on continuation (in terms of usage). Along this line, it appeared that convenience was the first triggering element to convince users.

We can precisely notice, that in our case the way usefulness has been defined, concurs with the perceived benefits that Ryu (2018, p. 560) mentioned. The second element that is interesting is what Ryu (2018, p. 561) underlined, that there are differences based on the user type. In his study, users were classified as early vs late adopters. Ryu (2018, p. 561) found that convenience was primarily important for early adopters, while late adopters regarded the economic benefits as more important. In essence, it appears that early adopters seek efficiency while late adopters seek economic gains. Moreover, the difference in terms of perceived security could be explained by the fact the early adopters may believe that the technology is reliable while their peers are sceptical (Ryu, 2018, p. 561).

The classification of users could be explaining the differences in terms of perceptions and thereby the results we have. In that sense, even though the binary logistic regression only delimitates the respondents in terms of users of non-users. The user’s type may be the reason why Perceived Usefulness was found affecting the usage, and we may induce that for the part of our respondents who were categorized as occasional users based on question 6 (in our survey) that their usage is contextual. The last interesting element of the logistic regression is that neither Organizational trust nor any of the sub dimensions of Perceived cybersecurity (i.e. Device security, Platform security and service security) were found to be affecting the respondent’s payment intention. In essence, the respondents did not perceive Organizational trust or Perceived cybersecurity to be important and that only the Perceived Usefulness is, meaning that the benefits of using mobile payment applications could be balancing the lack of security and trust. This result is similar to the results of Lim et al. (2018, p .8) who did not find that Perceived cybersecurity was affecting intention to use. Our result contradicts Steward and Jürjens (2018) who emphasized the importance of “Data security” and “Customer Trust”. In order to have a deeper insight of our sample and to create variance in terms of answers, we have decided to run a multiple regression analysis. It would be interesting to compare the results of the logistic regression with the multiple regression analysis.
7.3 Discussion about the multiple regression analysis on the conceptual model

The aim of the thesis is to investigate from a customer perspective the technological acceptance of mobile payment applications also known as FinTech payments, by considering the role of Perceived cybersecurity and Organizational trust. As a result, we have revised the Technological Acceptance Model (TAM) from Stewart & Jürjens (2018), by elaborating on the notion of “Data security” and by contextualizing the intention to use so that it converges with the online trust literature, which supports that trust should be understood as both trust in the technology and trust in the organization. As a result from our theoretical conceptualizations; we decided to test in a multiple regression analysis the following dimensions: Perceived Usefulness, Perceived Ease of Use, User Design Interface, Perceived cybersecurity (comprising four sub dimensions: service, platform, network and device security) and Organizational trust understood as reputation (itself sub classified as integrity, benevolence, and competence). Each of the dimensions has been previously categorized as factors based on the PCA which was run.

Service security has not been found to be statistically significant. Usability & ergonomics has been found to be statistically significant. Organizational trust found to be statistically significant. Device security has been found to be statistically significant. Perceived Usefulness has been found to be statistically significant. Platform security has not been found to be statistically significant.

We will now elaborate on the Perceived cybersecurity part. The first scholars to consider perceived security as defined as service security, platform security, network security and device security in the context of FinTech are Lim et al. (2018, p. 4). Lim et al. (2018) originally postulated the extended post acceptance model or (EPAM), where part of their model was to test whether perceived security is affecting continuous intention of FinTech. Lim et al. (2018, p. 8) concluded that perceived security is indeed of high importance and well specified by the four dimensions that is service, platform, network and device security. Lim et al. (2018, p. 8) also underlined that fact that each of the dimension as actually affecting the perceived security in FinTechs. Nevertheless, perceived security was not found statistically significant towards continuous intention to use.

Our results are quite similar to the one of Lim et al. (2018, p. 8). Even though we were expecting to see that each of the Perceived cybersecurity elements would have an impact on the intention to use. It appeared that in our case, the network security was not even eligible for further testing, while out the three dimensions remaining only one has been found to be statistically significant. For instance, the service security variable which was defined by the following statement:

AS1: Do you think the payment processes are secure?
AS2: Do you think the user authentication processes are secure?
AS3: Do you think the user's data is confidential?
AS4: Do you think the user access control (e.g. BankID) is verified?

It appears that the security related to the mobile application itself does not represent a barrier or even affect the intention to use of our respondents.
Along this line, the platform security dimension was defined by:

TS1: Do you think when using mobile payment apps, the operating system is secure?  
TS2: Do you think when using mobile payment apps, the platform is secure?  
TS3: Do you think when using mobile payment apps, the platform is maintained and repaired periodically?

It appeared once again that the technology behind mobile payment application is not affecting their intention to use. What is interesting, is that our results are mostly in accordance with the one of Lim et al (2018, p.8), yet the dimension of device security is the one that has been found to affect the intention to use of our respondents. Device security was tested with the three following questions:

SmS1: Do you think your mobile is secure?  
SmS2: Do you think your mobile is sufficiently performing to support the use of the mobile payment services?  
SmS3: Do you think, your mobile was supplied by a trusted/certified salesperson?

It is important to note the following facts; the questions which were asked to the respondents were technical or related to a certain knowledge related to IT. The questions were designed to include the most important elements that constitute the security in the IoT, as Sicari et al. (2015, p. 148) mentioned the relevance of three key security requirements that are: authentication, confidentiality and access control. Looking into the specification for each statement from a descriptive perspective might allow us to better interpret the cause of the results.

Most respondents for the questions AS1, AS2 and AS4 selected “I agree” which indicates that most have a positive attitude towards those aspects and expect their service providers to be secure. Question AS3 was answered mostly with “neutral” indicating that many do not particularly think that their data is confidential. Service security has been found not to be statistically significant and thereby not affecting the respondent’s intention to use of mobile payment applications. Nevertheless, what could explain that in general respondents are inclined to have a positive perception of the service they are using yet feel undecided about the privacy and security of their data? We have previously explained that in the context of mobile payment applications and thus by extension FinTech that the online trust literature was essential in order to comprehend what could influence technological acceptance or not. We have defined Organizational trust based on a reputation which is then comprehended by three major dimensions: integrity, benevolence and competence (Mayer et al., 1995). We discarded the competence dimension as it was not loading correctly based on the PCA. However, the two other dimension of trust was defined the following way:

I1: Do you think the mobile payment providers (companies) are trustful?  
I2: Do you think the mobile payment providers (companies) are honest?  
I3: Do you think the mobile payment providers (companies) keep their commitments?  
Be1: Do you think the mobile payment providers (companies) act in my interests?  
Be2: Do you think the mobile payment providers (companies) are helpful?  
Be3: Do you think the mobile payment providers (companies) are interested in my opinion?
We presume that the concept of Trust could be at the core of the explanation. This assumption is also motivated by the fact that according to our multiple regression analysis, the factor representing Organizational trust has been found significant. Could we explain the fact the service security is not affecting the intention to use of the respondents by the fact that their trust in the organizations providing such services does? In fact, looking at the trust literature and more specifically the online trust literature, we have already mentioned that trust is a multidimensional concept. As such, trust was broadly categorized in three main theories or movements: trust as personality theory, risk expectation theory and institutional theory.

One plausible explanation would be that respondents assume that the mobile payment applications used are secure. In order to motivate such assumption, the considerations of two elements are essential: first of all, and as mentioned by Freij (2018), there is an exponential intensification in terms of frequency and impact of regulations onto the financial industry. These regulations are recently targeting topics such as information security with for instance the directives GDPR or PSD1/PSD2. The increasing importance to the topic might support the illusion of a safe regulatory environment and therefore contribute to the respondent’s belief that the mobile payments apps are secured. Secondly, the institutional theory of trust could give us more insight by implying that the trust the respondents had in the organizations is clearly affecting their intention to use the service. Viewing trust as an institutional phenomenon clearly extends trust interactions, where trust is extended from an individual to an organization (Lewiki & Bunker, 1996, p. 119).

Consequently, the respondents would value and place their trust in the organizations regardless of the security measures taken by the organizations. It would eventually mean that the factor which was describing Organizational trust (i.e. constructed on the benevolence and integrity attributes of the service providers) and which was built on reputational attributes may have a bigger impact on the intention to use than the actual security of the services provided. For instance, it was argued by Kryparos (2018, p. 43) that trust in the financial institutions has been established by years of consistency in delivering promises by fulfilling customer’s interests.

Could it be that mobile payment applications were able to build credibility and reputation by answering to customer’s needs and exhibiting transparency about the service they offer? This also corresponds with what we discussed in the literature review, where we stated that internet services nowadays enjoy a high degree of trust although it is a recent phenomenon compared to other industries. No one questions the integrity of for example amazon and almost everyone is willing to buy things online nowadays (Lewan, 2018, p. 117). Yet, the results about service security are contradicting the study of Stewart and Jürjens (2018, p. 123), who stated that data security is the one of the most relevant aspect in the adoption of FinTech services. Stewart and Jürjens (2018, p. 123) precisely argued that consumers possess expectations regarding their personal data and as such expect it to be secure, especially as the consumers are aware of the different data breaches currently occurring within the industry.
For instance, Stewart and Jürjens (2018, p. 123) argued that, through the media and social networks, most people are aware of the increased amount of cyber-attacks on bank networks and that they are aware about how little has been done. Therefore, consumers value their data and make data security an important aspect in adopting Fintech services. Our result however indicates that people are aware that Fintech handle their data are probably not confidential but do not really think about it when deciding to adopt a service or not.

This is probably due to the fact that it is widely known that most services use data and that data confidentiality and security never can be fully guaranteed. This result is confirmed by Lim et al. (2018, p. 6) who argued that perceived security (which includes platform security) does not show a direct effect on the satisfaction and continuous intention to use the services of consumers. The results we have, namely the fact there is a positive relationship between Organizational trust and Intention to use of mobile payment apps is also supporting the results of Stewart and Jürjens (2018, p. 122). In this line, Stewart and Jürjens (2018, p. 122) stated that customer trust is fundamental and that its absence would result in hindering FinTech’s adoption.

Lastly, it is interesting to balance our results by taking into consideration the answers of our respondents on the trust element. While most respondent think that mobile payment providers are trustful and helpful, there are many who think that mobile payment providers do not act in the interests of the customer and are dishonest. This might be explained by individual’s characteristics regarding trust, to the extent the individual’s propensity to trust.

The last element we would like to elaborate on regards the results we obtained for the dimensions: Perceived Usefulness, Usability & ergonomics and lastly device security. First of all, we would like to mention that most respondents in our study have a strong intention to use a mobile payment application and that 92% of them are actually carrying out payment transactions with at least one of them. Yet, our respondents are not aware of the terminology FinTech. It therefore means that from a Fintech perspective it would be beneficial for companies to advertise more on what they are doing so that people are capable of associating them with the new taxonomy. Our results also show that usability & ergonomics, device security and Perceived Usefulness are statistically significant and have a positive relationship with the intention to use mobile payment apps.

Perceived Usefulness was assessed based on the following statements:

U1: Do you think mobile payment apps are convenient?
U3: Do you think mobile payment apps are fast?
U4: Do you think mobile payment apps are available as a payment method?

Perceived Usefulness has been defined around three notions which are convenience, responsiveness and availability. It is clear that all of these notions are contributing to what is called the beneficial aspect of mobile payment application. As such, our results are similar to the ones of Ryu (2018) who found that the benefits: such as economic benefit, seamless transaction and convenience were statistically significant and had positive relationship with continuance to use FinTech.
We can precisely notice, that in our case the way usefulness has been defined, concurs with the perceived benefits that Ryu (2018, p. 560) mentioned. Additionally, our results coincide with the ones of Lim et al. (2018, p. 9) who tested whether usefulness had direct impact onto satisfaction and continuous intention. Even though Lim et al. (2018) original intent is different from ours, the scholars have proven importance of usefulness onto the continuous intention.

In contradiction, Stewart and Jürjens (2018) whose study is highly similar to ours found that Perceived Usefulness was not affecting the customer’s intention to use FinTech. So, what could explain the fact Perceived Usefulness is affecting the intention to use? In order to answer to provide a plausible answer to the interrogation, it is necessary to consider the trust literature and its impact on the intention to use. Part of the trust literature exposes that trust can be theorized from a risk expectancy perspective.

As we have previously mentioned based on Blau (1964); trust is to be a crucial feature in both the introduction and maintenance of social relations. Along this line, Barber (1983) expressed three types of expectations resulting from trust which he described as 1) expectation of persistence and maintenance of social order 2) expectation of the technically competent role performance from those involved in individuals’ social relationships and lastly 3) expectation that participants within the interaction will execute their economic and moral obligations or responsibilities. In our case, we are interested in the respondent’s expectations about the competency and performing role of the service providers as well as the service itself being capable of answering our respondents’ needs.

Subsequently, the fact Perceived Usefulness was found to affect their intention to use the mobile payment apps could be explained by the latent expectations that the respondents have towards the service itself. As the service appears to be useful to them in terms of convenience, responsiveness and availability, we could induce that it reveals reliability about the mobile payment applications used. Therefore, trust is met since the respondents consider the mobile payment applications to be up their expectations. Moreover, we should not forget that Organizational trust has also been found to affect the Intention use, thereby supporting the idea that the trustor’s perception of the trustee (the respondent’s perception of the service providers: companies providing payment apps) is honest. In other words, the self-protection made by the respondents about the service providers’ trustworthiness, pinpoints that trust is mostly relying on the respondents’ ability to assess the reliability of the service providers.

As we are dealing with a service that is based on a transactional perspective; trust is usually extended by including dimensions such as reputation, performance and appearance (Sztompa, 1999). We may induce that Perceived Usefulness is indeed linked to the performance aspect of the mobile payment application but also to the reputational attribute of the service providers which both have been found to be statistically significant in our study. As a result, trust plays a significant role for either the continuation or completion of the exchange (James, 2002, p. 293).

The second element which has been found to be important in our study is the effect of usability and ergonomics. The dimension Usability and ergonomics has been delimited after running the principal component analysis and as such the dimension includes the following elements:
D1: Do you think mobile payment menus are easy to navigate?
D2: Do you think mobile payment menus are understandable?
D3: Do you think mobile payment menus are easy to use?
E2: Do you think mobile payment apps provide me guidance?
E3: Do you think mobile payment apps are user friendly?

The positive relationship between usability & ergonomics and the intention to use mobile payment apps and Perceived Usefulness and the intention to use mobile payment apps indicate how important it is to create a high usability for the apps. If consumers understand the app and know how to use it, they are much more likely to adopt the mobile payment app. This result corresponds with the result of Egger (2002, p. 40) who states that attractiveness and a high usability increases the willingness of customers to explore products.

As well as with the result of Stewart & Jürjens (2018, p. 122) who state a poor User Design Interface as one of the principal hindrances of FinTech innovation and Yang, H.-d., & Yoo, Y. (2004, p. 273) who state that Perceived Usefulness influence the attitude toward using mobile commerce. Considering that Swish and Klarna are the two mobile payment applications which are the most represented amongst our respondents we could extend that those services have a high usability, good ease of use and a good design. Once again, trust as expectations could be explaining why features such as usability and ergonomics are of high importance for our respondents. The fact that usability is enforced by ease and design supports the idea that User Design Interface is an antecedent of trust which in return supports Beldad et al. (2010, p. 861). In other words, they are the antecedents affecting the behavioral customer’s intention to adopt FinTech services (Beldad et al., 2010, pp. 861-867).

The last point we would like to address is dealing with the results we have for the device security. In our study, device security has been found to impact the intention to use. Device security is the only of the four perceived security dimensions which has been found to be significant. What could explain the fact our respondents felt that their device security would affect whether or not they would be using a mobile payment application. We could hypothesize the following, namely that the device security is the closest dimension of security that the respondents are in contact with. In essence, when they are carrying out a payment transaction, they are usually doing it from their smartphone, and as such, the fact that their smartphone is considered secured could explain why they trust it to carry out the payment.

Therefore, proximity as security could be explaining why device security is important. Furthermore, the fact that the mobile payment application is used on their smartphone supports the convenience of the service. Thereby device security in combination with Perceived Usefulness and trust in the organization providing the application could explain its effect on the respondent’s intention to use. The online trust literature provides a valuable insight by considering trust from a psycho sociological perspective. In fact, trust is assimilated to a confident attitude that the no one will use one’s vulnerability against; to the extent it is accepting the risk related to the interaction (Corritore et al., 2003).
Yet, we have mentioned that the primary difference between offline and online is the context but also the object of trust which is thus extended to the mean of exchange and the organization deploying the technology (Shankar et al., 2002). Could it be that the respondents because they own the smartphone, because of its proximity and reliability and the fact that trust the organizations would result in engaging into carrying payment transactions as it is convenient? According to our study, it appears that users are most likely interested in the beneficial aspect of the mobile payment applications rather than its security. Yet, the Perceived Usefulness characteristic tends to emphasize the notion of reliability and therefore security. The dimension of organizational trust plays a major role in the interaction with mobile payment apps. Organizational trust could be explaining many of the reasons why respondents felt safe using online application payment services. Trust is present in every aspect of the transactions, whether it is in shaping the respondent’s expectations and therefore affecting their view of usefulness, usability and ergonomics or by highlighting the trust in the institution behind the service. It is interesting to notice that the results are different than the one we obtained from the binary logistic regression. In a situation where respondents have only the choice between carrying or not carrying payment transactions with a mobile payment app, it suggested that only device security and Perceived Usefulness matter.

7.4 Discussion about the multiple regression analysis with overall security and trust.

As part of our questionnaire, we decided to also ask two questions which would be addressing the concepts of security and trust. As a result, the first question we asked our participants was to rank their overall experience in terms of security when using mobile payment applications. In order for respondents to fully understand the ins and outs of the question we have mentioned that security would be including service security, platform security, network security, and device security. Lastly, we intentionally warned the respondents that if one of the dimensions we mentioned was not safe then the entire security of the transaction could be compromised. The second question was assessing the concept of Trust, by asking respondents to rank their trust in the companies which are providing mobile payment applications. From these two questions and with our question assessing the “intention to use”, we have decided to run a multiple regression analysis. Overall security and trust were the predictors of “intention to use”. Overall security has been found to be statistically significant. Overall trust has been found to be statistically significant. We obtained a statistically significant relation of both overall security and overall trust to our dependent variable which is intention to use mobile payment apps.

It is interesting to notice, that in comparison to the previous multiple regression analysis, this time both overall trust and security matters. In essence, the concepts of Trust and Security have a positive effect on the Intention to use. Many studies have outlined the importance of either security or trust in respect to technological adoption (Wang et al., 2003; Luarn & Lin, 2005; Liu et al; 2009; Liao et al., 2011 cited in Gai et al., 2018; Stewart & Jürjens, 2018). Nevertheless, it is also surprising that overall security is significant in this regression but was not when conceptualized by service security, technology security and device security.
This peculiar observation could be explained in two ways: first, over identifying the concept of Perceived cybersecurity may have undermined its importance and the risk it represents in reality; secondly security has been defined based on overall experience. Consequently, if the respondents did not have a bad experience it can shape their view on the service they are using, and therefore it reinforces the fact that benefits might win over the risk aspect. Lastly, we intentionally decided not to include any control variables such as Perceived Usefulness, Usability & ergonomics; as both overall trust and security were measuring a different concept than Perceived cybersecurity or Organizational trust.
8. Conclusion

8.1 Conclusion

We intended to answer to the research question: What is the role of Perceived cybersecurity and Organizational trust on the customer’s intention to use mobile payment applications?

In order to provide a meaningful answer to this question, we have decided to run three regression analyses. The first one was a binary logistic regression, which was supposed to shed the light on whether the respondents of our study are carrying out payment transactions through a mobile payment application. The dependent variable was thus their payment intention and the independent variables were the variables which have been extracted from the Principal Component Analysis (PCA) with an oblique rotation.

In other words, the different variable used to explain the payment intention is Service security, Usability & ergonomics, Perceived Usefulness, Device security, Organizational trust (i.e. benevolence and integrity) and Platform security. Based on binary logistic regression, the results suggested that only Perceived Usefulness and device security had a positive and statistically significant effect on the respondent’s payment intention. We hypothesized that users who considered their phone secure did not necessarily see more risks in using a mobile payment app and were more likely to carry out the payment transactions based on its beneficial attributes. To support such argument, we referred to Ryu (2018), who investigated what makes users willing or hesitant to use FinTech. In his model which was centred on the Theory of Reasoned Action (TRA), Ryu (2018) developed a benefits risk framework based on: economic benefit, seamless transaction and convenience. Additionally, Ryu (2018) found that the three were statistically significant and positive with continuance to use FinTech. To some extent, our results converged with the ones of Ryu (2018, p. 560) where he concluded that in general perceived benefits have a stronger impact on continuation (in terms of usage). Along this line, it appeared that convenience was the first triggering element to convince users. We can precisely notice, that in our case the way usefulness has been defined, concurs with the perceived benefits that Ryu (2018, p. 560) mentioned. The second element that is interesting is what Ryu (2018, p. 561) underlined, that there are differences based on the user type. As a result, we have hypothesized that user type or classification may influence their payment intention.

The second analysis was a multiple regression one, where we decided to use the customer’s intention use defined based on our online survey (question 6) and use the same independent variables as in the binary logistic one. Table 11, which is the robust multiple regression on our model suggested that:

1. Service security has not been found to be statistically significant.
2. Usability & ergonomics has been found to be statistically significant.
3. Organizational trust has been found to be statistically significant.
4. Device security has been found to be statistically significant.
5. Perceived Usefulness has been found to be statistically significant.
6. Platform security has not been found to be statistically significant.
Based on Table 11 we were able to derive the following equation:

\[
\text{Intention to use} = 3.811 + 0.175 \times (\text{Usability & ergonomics}) + 0.202 \times (\text{Organizational trust}) + 0.116 \times (\text{Device security}) + 0.388 \times (\text{Perceived Usefulness}) + \epsilon
\]

We presume that the concept of Trust could be at the core of the explanation as argued in the discussion section 7.3.

Lastly, the final regression which was conducted was primarily aimed at testing whether trust and security, if regarded as overall concept could be explaining our respondent’s intention to use. The results suggested that both overall trust and overall security were positively significant and affecting the respondent’s intention to use.

In conclusion, to the question: what is the role of Perceived cybersecurity and Organizational trust on the customer’s intention to use mobile payment applications? We could answer that based on our respondents and the statistical analyses performed that both Perceived cybersecurity and Organizational trust matters but at different levels. We must balance our results as we have conducted three regression analyses. Our results suggest that the payment intention of our respondents (binary logistic regression) is primarily motivated by the Perceived Usefulness and the Device security. As such, we could hypothesize that the results suggest the predominance of the benefits in terms of usefulness over security, yet security only appears to be valuable in the form of Device security. The second regression provides a deeper insight by confirming that the intention to use is primarily affected by Perceived Usefulness, Usability and ergonomics, Device security and Organizational trust. As such, we can only conclude that the benefits are once again highly valuable yet trust in the organization providing the services could be explaining why not all the dimensions of Perceived cybersecurity are important. It almost suggests that the combination of highly beneficial attributes and trust in the service providers are enough to make the user feel safe about the service he/she is using, as it is reliable. Nevertheless, the third regression emphasizes that if security and trust are regarded as englobing concepts, namely not divided into subcategories, that both are essential to explain the intention to use of our respondents. In essence, Perceived cybersecurity and Organizational trust are antecedents of mobile payment applications and customer’s intention to use. Yet trust in combination with beneficial attributes may be enough to ensure usage.

8.2 Research implications

8.2.1 Theoretical contribution

As we have previously mentioned, the advent of the Information and Communication Technologies is mostly referred to “digitalization”, and as such it offers a new paradigm. Information technology is regarded as a disruptive innovation currently shaking up the traditional financial industry. Because of the former trend, a new taxonomy emerged under the name of “FinTech”, corresponding to the embracement of “digitalization”. FinTech is disintermediating through innovation.
Peculiar incidents at the macroeconomic level whether in the form of financial crisis or cyber-criminality, have profoundly reshaped the regulatory environment. The inevitable changes occurring at a higher pace in terms of consistency and significance led to disrupt and create a favorable regulatory environment currently driving innovation within the financial industry. Even though the changing regulatory environment firstly acted as a catalyst by promoting the FinTech phenomenon into the spotlight, it inherently touched upon one of the prominent challenges of “FinTech”: to the extent Information Security.

Ultimately, FinTech’s ecosystem symbolized by the “Always Available” expression conveys an explicit statement which is yet challenged by the threat of cyberattacks. In fact, in this thesis, we argue that Innovation is conveyed by FinTech’s and their ability to innovate through disintermediation; by proposing tailored technologically driven solutions responding to undermined consumer’s needs. Yet, the new perspective given by this “FinTech” phenomenon is confronted to a paradox. A dilemma which is stated as the existing tension between their promises to be “always be available” and at the same time “be secured”. The existing paradox reasserts the growing need for trust from a customer perspective.

To the extent, the duality extends to portray the FinTech’s penultimate challenge which is the need to build a trust mechanism while ensuring security. Ensuring security and trust is perceived to be one of the reasons why consumers are reluctant to shift to the non-traditional financial service provider. Consequently, the presupposed interrelation between information security and trust in the context of FinTech could constitute the solution for promoting technological acceptance amongst consumers. In this thesis, we argued in the line of Stewart and Jürjens (2018, p. 113) who explicitly indicated the need to: “highlight the necessary perspectives for the FinTech adoption process”. Subsequently, we acknowledged the need to include two dimensions of high significance for the FinTech phenomenon: namely the impact of information security and trust onto the technological acceptance. Scholars have mentioned that information security and trust appeared to be crucial for FinTechs (Liao et al., 2011 cited in Gai et al., 2018, p. 263). Plus, different studies have outlined the importance of either security or trust in respect to technological adoption (Wang et al., 2003; Luarn & Lin, 2005; Liu et al; 2009; Liao et al., 2011 cited in Gai et al., 2018; Stewart & Jürjens, 2018). The major divergence with prior researches results from the conceptualizations of both information security and trust.

As a result, we have decided to elaborate on the Technological Acceptance Model (TAM) by implementing the dimension of security and trust. In essence, we have decided to extend and adapt the model of Stewart and Jürjens (2018) by defining both their variable of “Data security” and “Customer trust”. By shedding the light on the deficiencies of the various theories addressing the technological acceptance; we have decided to further elaborate the research model of Stewart and Jürjens (2018). Their model originally comports five dimensions respectively Data Security (DS), Customer Trust (CT), Value Added (VA including Perceived Usefulness (U) and Perceived Ease of Use (E)), FinTech Promotion (FP), and User Design Interface (UI). Based on Stewart and Jürjens model about FinTech acceptance model (2018), we postulated a different conceptualization of both “Data security” as “Perceived cybersecurity”. Lim et al (2018, p. 3), conceptualized perceived security of FinTech as a multidimensional construct.
The main argument for applying a multidimensional view on perceived security emanates from the fact that security is a mechanism which needs to be applied at numerous levels whether in the form of physical methods or application-based ones (Lim et al., 2018, p. 3; Gai et al., 2018, p. 264). Lee (2015) stressed out the different layers including service security, platform security, network security and device security which are conceived as essential elements of the Internet of Things.

Yet, we have not labelled it as perceived security, but Perceived cybersecurity based on the section 2.2.2. Finally, we have decided based on the trust literature that trust as an expectation and trust as an institutional phenomenon convey the appropriate characteristics to converge with the online trust definition. Online trust allows us to consider not only the mean of exchange but also the organization providing the technology.

In other words, online trust is characterized by trust in the technology and trust in the organization providing the technology. Consequently, Stewart & Jürjens (2018) “Customer trust” variable has been interpreted as trust in the technology therefore converging to “Perceived cybersecurity” and trust in the organization (Organizational trust) has been defined in terms of: reputation understood as ability, integrity and benevolence (Mayers et al., 1995).

8.2.2 Managerial contribution

From a practical perspective, this thesis aimed to emphasize the role of Perceived cybersecurity and Organizational trust on the customer’s intention to use mobile payment applications. The study investigated based on a revised version of the Technological Acceptance Model Theory, what are the antecedents of intention to use. The study suggests that trust in the form of Organizational trust is relevant and affecting customer’s intention to use. Moreover, the study suggests that dimensions such as Perceived Usefulness, Usability and ergonomics are affecting customers’ intention to use. This knowledge is valuable for FinTech start-ups that would be developing a product or service related to a mobile application. The study aims to provide a valuable insight by identifying the elements and suggesting an interpretation of the results, which would be useful for the FinTech companies. Trust is the key to technological acceptance, and it can attain by different ways; our study suggests that the benefits of the service used and the reputational attribute of the company providing the service may be the answer to provide security. We firmly believe that developing trust inherently affect security and benefits the service in terms of usefulness.

8.2.3 Societal and ethical aspects

In this section, we would like to present the different considerations that have been taken in order to deal with societal, social or even ethical aspects during this thesis. The first element that we want to mention is that during the research process we decided to follow a certain number of rules in regard to the aim of our study. In essence, as we were conducting an online survey, we intended to respect the following ethical aspects: 1. No harm to participants. 2. No lack of informed consent. 3. No invasion of privacy. 4. No deception.
All participation in our survey was made on a voluntary basis. We explained the aim of the study to the respondents and also mentioned that they will remain anonymous. The only issue we could have generated is the way we have communicated our online survey, namely by collecting their email addresses from the University and sent them an email without their permission. Nevertheless, we decided to send the emails so that no other respondents could see who was receiving the mail. This was done thanks to the Bcc option in Gmail.

The last element that we would like to address is the social or societal impact of our study. The thesis sought to investigate what is the role of Perceived cybersecurity and Organizational trust on the customer’s intention to use mobile payment applications. As such, we would like to mention that everyone should be careful with the interpretation of our results. Our results which are both confirming the need for security and trust in order to influence customers and the fact that beneficial attributes are sufficient to influence customers may be wrongly interpreted. The participants in the FinTech ecosystem should use our results in an ethical manner by not falsely falling into the category where their only aim is to be perceived secured but not actually be secure. The same applies for trust. Each participant within the FinTech ecosystem should understand the value of security and trust and do not fall into a branding strategy which would falsely convince potential users of the security of the service provided. In essence, trust should be built on factual elements and not simply on an advertising campaign.

8.2.4 Limitations

We acknowledged different limitations regarding this thesis. The limitations have been divided into three broad categories: limitations regarding the theoretical ground, limitations regarding the statistical analysis, and limitations regarding interpretation.

The first limitation that we acknowledge is relying on the fact that we have postulated and anchored our study around a revised version of the Technological Acceptance Model (TAM). Our conceptual model even though novel may also represent a limitation as we could have defined trust in a different manner. Furthermore, in our theoretical frame of reference, we acknowledged the existence of different theories that are dealing with technological acceptance. A different conceptualization or different theoretical point of departure can be suggested, as for this thesis we were limited in terms of time and resources available.

The second limitation, we would like to address is pinpointing the collection of data. In this study, we have decided to use a convenience sampling and as such the sampling characteristics are limitations to the study as it is not a random probability sample and that it influences the generalization of the results. Part of the second limitation, the number of respondents can be considered as a limitation in comparison to the sample size. Lastly, the convenience sample might have overrepresented a specific category of the population (i.e. individuals at a higher education level proficient in English) which in itself forces us to balance our results and only mention that they are valid for our respondents.
The third limitation of this thesis is the lack of control regarding the variable propensity to trust. We have mentioned that trust is also a personality trait feature and that experience may affect our perception of trust. As such the fact that the study is not formerly trying to control for this element and that the study is conducted in Sweden may suggest that the cultural dimension affect trust.

The fourth and last limitation we would like to address is the type of statistical tests which were performed. These tests were selected in order to clearly explain the effect of each antecedent in regard to intention to use. Yet, in these tests, we did not take into consideration that security and trust may be interrelated and as such different approach could be suggested such as using structural equation modelling thereby allowing covariance within the concepts. A different approach to our data, namely the eventuality of a non-linear relationship or better fitted model had not been pursued.

8.3 Future Researches

The aim of this thesis was to investigate from a customer perspective, the technological acceptance of FinTech payment solutions by considering the role of Perceived cybersecurity and Organizational trust. As such, we advocate that future researches could replicate the study by first changing the sampling method to a random sample in order to counter the lack of generalization we are facing with the current study. Furthermore, in order to confirm our results, it would be beneficial to conduct a longitudinal study either in Sweden or by extending it to different countries. It would also be interesting to conduct a mix method study in order not only test which are the antecedents but also explore the causes or reasons why.

Additionally, a revision of the theoretical ground could be done by deepening the scope of the mean of exchange. In other words, looking into the online perspective and online trust perspective and its implications in the context of mobile payment applications could provide a better understanding and model to explain the customer's intention to use. Future researches could also extend the study of Perceived cybersecurity and Organizational trust in the context of a different FinTech branch. Finally, considering the interrelation between trust and security, it could be interesting to practically analyze companies and their strategies to develop the two former elements.

8.4 Truth criteria in social research

The three most important criteria for the evaluation of social research are reliability, replicability and validity (Bryman, 2012, p. 46).

8.4.1 Reliability

Reliability is assessing if the outcome of a study would be the same if the study would be repeated exactly the same way or if the outcome of a study is affected by random or temporary factors (Bryman, 2012, p. 46). Therefore, it is important that we consider this while conducting our study. In order to ensure reliability in our study, we first decided to ground our conceptual model on existing academic literature. The literature has been selected in order to support our conceptualization of the topic and its challenges. Each variable that has been selected was based on existing literature and each of the questions in the survey was developed in relation to existing questionnaire about the variables.
We simply adapted to the context of mobile payment applications and chose the wording in a careful manner based on a pilot study. The second element where we ensured reliability is the data.

We have conducted an online survey from which we gathered data. As the data is considered as primary data, it was essential for us that we provided the best reliability possible. As a consequence, we have first run a principal component analysis to confirm whether or not our data was correctly loading and representing the constructs we expected from the literature review. Each factor which was extracted was based on a certain amount of statements which we have decided to test for reliability by analysing their Cronbach’s alpha. We analysed the results of our questionnaire with the programs Excel, SPSS and STATA. All of them are considered to have a high credibility and quality for analysing data and are available to everyone. We controlled our statistical tests carefully for human error.

8.4.2 Replicability

In order to ensure replicability, we have tried to explain all the steps that have been taken and motivate them so that anyone could understand. Furthermore, all the results are provided either within the text or in the Appendixes. We have also made sure to enclose the questionnaire, if future researchers would be interested in conducting a similar study. Lastly, we will be providing our email addresses so that we can share the raw data with everyone who would be interesting in either checking the validity of our results or compare their results with ours.

8.4.3 Validity

Validity is concerned with the integrity of the conclusions that are drawn from the research. Validity is achieved if the conclusions of the research are connected to what the research planned to find out. There are different types of validity. The first one is measurement validity which means that the variables in the study really measure what they intend to measure (Bryman, 2012, p. 47). In our case, we made sure that measurement validity was valid by basing our questionnaire on existing literature and conceptualizations; by checking the what we measure with our questions actually is what we want to measure (e.g. we have used the factor analysis with the principal component analysis to do so). The second type of validity is internal validity and is concerned with whether a conclusion that incorporates a causal relationship between two or more variables is sustainable (Bryman, 2012, p. 47). In our case the internal validity was taken care of by carefully applying the statistical rules and procedures regarding the tests conducted. Namely, we measured internal consistency and therefore validity by checking the Cronbach’s Alpha of our constructs. We also have discarded the dimensions which did not meet the criteria to run further tests. We made sure that each of our decision was motivated both theoretically speaking but also statistically, for example retaining only factors with an eigenvalue over 1. The only element that could be improving that matter would be to perform a parallel analysis in order to confirm that 6 variables needed to be extracted. The parallel analysis simply will compare by randomly creating the same data set as the original data and will calculate the eigenvalues for each of the elements. The eigenvalues from the data set and the Montecarlo simulation will be compared and we will retain the only ones that are considered not be determined by random luck.
The third type of validity is called external validity and is concerned with whether or not the results of a study can be generalized to other research in the same field of research (Bryman, 2012, p. 47). As we have conducted our study based on a convenience sample, the external validity is lower than if it would have been based on a random sample. Therefore, our study is lacking generalization and the results are only applicable to students at Umeå University. Lastly, we want to mention that all the interpretations of the results are made and should be balanced by our sample characteristics and that the discussions around the results are made in accordance with our critical realism stance where we intend to be objective yet suggest interpretations of the results based on the literature.
Reference list


ISACA (2016). ISACA CSx Cybersecurity Fundamentals. Available at: https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Elgnatuschtschenko_GCSSC_preseation_160112_0.pdf


Lewicki, R.J., & Bunker, B.B. (1996). Developing and maintaining trust in work relationships In:


Verizon, 2016. 2016 Data Breach Investigations Report: 89% of breach had a financial or espionage motive. [electronic]. Available via: https://regmedia.co.uk/2016/05/12/dbir_2016.pdf [Retrieved February 27, 2019]


Appendix 1: Questionnaire.

**Survey: Information security and trust.**

As part of our graduate program, we are conducting a social sciences research related to finance. We are interested in your perceptions of information security and trust regarding mobile payment apps. We kindly ask for your voluntary participation in this survey. It will take approximately 5 minutes. If you decide to fill in the survey, you get the chance to win a gift card for Filmstaden of 250 SEK. All answers will remain confidential.

Thank you for the valuable time you will spend in completing the survey.

Best Regards,
David and Robin.

*Required

**Email address** *

**Demographics**
This section is intended to gather information about the respondents. N.B: All information will remain anonymous.

**Q1: Please indicate your gender.** *
*Mark only one oval.

- ○ Male
- ○ Female
- ○ Other

**Q2: Please select your age category.** *
*Mark only one oval.

- ○ 18 to 24
- ○ 25 to 31
- ○ 32 to 38
- ○ 39 to 45
- ○ 45 +

**Q3: Which faculty do you belong to?** *
*Mark only one oval.

- ○ Faculty of Arts
- ○ Faculty of Medicine
- ○ Faculty of Social Sciences
- ○ Faculty of Science and Technology
FinTech
In this section, we purposively do not define the word FinTech in order to see who is aware or not of the phenomenon.

Q4. Are you aware of the word "FinTech"? *
Mark only one oval.
- ○ Yes
- ○ No

Q5. Are you using a mobile application related to a financial service? *
Mark only one oval.
- ○ Yes
- ○ No
- ○ Maybe

Q6. Intention to use a mobile payment app? *
Mark only one oval per row.

<table>
<thead>
<tr>
<th>Very Low</th>
<th>Low</th>
<th>Occasionally</th>
<th>Strong</th>
<th>Very strong</th>
</tr>
</thead>
<tbody>
<tr>
<td>I intend to use a mobile payment application</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Q7. Do you carry out payment transactions with a mobile app? *
Mark only one oval.
- ○ Yes
- ○ No

Q8. Which mobile payment service are you using? *
Tick all that apply.
- □ Swish
- □ Klarna
- □ Gpay
- □ Apple pay
- □ Samsung Pay
- □ Paypal app
- □ Alipay
- □ Wechat pay
- □ Others
- □ None
**Benefits of FinTech**

In this section, several statements will be given to test different elements. Please select your degree of approval. READ CAREFULLY: FinTech definition: it is a short for financial and technology. It describes companies offering technology based solutions for finance. Most common example would be mobile payment applications: e.g. swish, klarna, gpay etc.

**Usefulness** *

*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think mobile payment apps are convenient.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think mobile payment apps are reliable.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think mobile payment apps are fast.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think mobile payment apps are available as a payment method.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Ease** *

*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think mobile payment apps are clear.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think mobile payment apps provide me guidance.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think mobile payment apps are user friendly.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Design** *
*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think mobile payment menus are easy to navigate.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Do you think mobile payment menus are understandable.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Do you think mobile payment menus are easy to use.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**Information security**

In this section, several statements will be given to test different elements. Please select your degree of approval. READ CAREFULLY: FinTech definition: it is a short for financial and technology. It describes companies offering technology based solutions for finance. Most common example would be mobile payment applications: e.g. swish, klarna, gpay etc.

**How would you rate your overall experience of mobile payment applications in terms of security? ** *

Security includes the following aspects: app, the technology behind the app, network, and the mobile. If one of the aspects is not safe, the risk of facing a security incident is higher.

*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very high</th>
</tr>
</thead>
<tbody>
<tr>
<td>I consider my overall experience in terms of security as:</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
</tbody>
</table>

**App security. ** *

When using mobile payment apps:

*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think the payment processes are secure.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Do you think the user authentication processes are secure.</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☐</td>
</tr>
<tr>
<td>Strongly disagree</td>
<td>Disagree</td>
<td>Neutral</td>
<td>Agree</td>
<td>Strongly agree</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------</td>
<td>---------</td>
<td>-------</td>
<td>----------------</td>
</tr>
<tr>
<td>Do you think the user's data is confidential?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think the user access control (e.g. BankID) is verified?</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Technology security** *

Operating system: for example Windows, iOS, Android etc. Platform security: refers to the overall security of a computing platform (e.g. hardware, software, network, storage etc.). If one of the aspects is not safe, the risk of facing a security incident is higher.

*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
<th>No opinion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think when using mobile payment apps, the operating system is secure?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think when using mobile payment apps, the platform is secure?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Do you think when using mobile payment apps, the platform is maintained and repaired periodically?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Network security** *

The security related to the network used (e.g. wifi, internet data) when using a mobile payment app.

*Mark only one oval per row.*
Do you think, the wireless networks are safe.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

Do you notice any network communication problems when using mobile payment apps.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

Do you think an immediate response is given in case of network failure.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

**Smartphone security.** *

Security related to smartphone while using the mobile payment application.

*Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

Do you think your mobile is secure.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

Do you think your mobile is sufficiently performing to support the use of the mobile payment services.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

Do you think, your mobile was supplied by a trusted/certificed salesperson.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>☐</td>
<td>☐</td>
<td>☒</td>
<td>☐</td>
</tr>
</tbody>
</table>

**Trust**

In this section, several statements will be given to test different elements. Please select your degree of approval. READ CAREFULLY: FinTech definition: the combination of the two terms Financial and Technology. It describes companies offering technology based solutions for finance. Often, the companies are not traditional financial service provider.

**How would you rate your overall trust in the companies providing mobile payment apps?** *

trust being defined as integrity, benevolence and competency
Mark only one oval per row.

My trust in the companies is:

<table>
<thead>
<tr>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
<th>Very high</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Integrity * **

Integrity: is defined as your perception about company providing the mobile payment app (person to be trusted)

Mark only one oval per row.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do you think the mobile payment providers (companies) are trustworthy.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do you think the mobile payment providers (companies) are honest.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do you think the mobile payment providers (companies) keep their commitments.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Benevolence * **

Benevolence: is defined as your perception about the company as not being profit driven.

Mark only one oval per row.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do you think the mobile payment providers (companies) act in my interests.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do you think the mobile payment providers (companies) are helpful.

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Do you think the mobile payment...
providers (companies) are interested in my opinion.

**Competency** *

Competency is defined as your perception about the company as having the skills, expertise in its business area. *Mark only one oval per row.*

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think the mobile payment providers (companies) are efficient in providing their services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Strongly disagree</th>
<th>Disagree</th>
<th>Neutral</th>
<th>Agree</th>
<th>Strongly agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you think the mobile payment providers (companies) have expertise in providing their services</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Appendix 2: Descriptive statistics.

<table>
<thead>
<tr>
<th>Statistic</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
<th>Std. Deviation</th>
<th>Skewness</th>
<th>Kurtosis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q6 Intention use</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.81</td>
<td>1.082</td>
<td>-.745</td>
<td>.057</td>
</tr>
<tr>
<td>U1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.51</td>
<td>.659</td>
<td>-1.248</td>
<td>1.683</td>
</tr>
<tr>
<td>U2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.81</td>
<td>.812</td>
<td>-.520</td>
<td>.280</td>
</tr>
<tr>
<td>U3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.49</td>
<td>.696</td>
<td>-1.449</td>
<td>2.569</td>
</tr>
<tr>
<td>U4</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.18</td>
<td>.770</td>
<td>-.798</td>
<td>.652</td>
</tr>
<tr>
<td>E1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.13</td>
<td>.754</td>
<td>-.923</td>
<td>1.788</td>
</tr>
<tr>
<td>E2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.71</td>
<td>.845</td>
<td>-.290</td>
<td>-.058</td>
</tr>
<tr>
<td>E3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.19</td>
<td>.744</td>
<td>-.807</td>
<td>.912</td>
</tr>
<tr>
<td>D1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.15</td>
<td>.753</td>
<td>-.922</td>
<td>1.769</td>
</tr>
<tr>
<td>D2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.15</td>
<td>.744</td>
<td>-.895</td>
<td>1.573</td>
</tr>
<tr>
<td>D3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>4.20</td>
<td>.731</td>
<td>-.892</td>
<td>1.571</td>
</tr>
<tr>
<td>AS1</td>
<td>361</td>
<td>2</td>
<td>5</td>
<td>3.81</td>
<td>.733</td>
<td>-.330</td>
<td>.010</td>
</tr>
<tr>
<td>AS2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.73</td>
<td>.861</td>
<td>-.660</td>
<td>.372</td>
</tr>
<tr>
<td>AS3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.14</td>
<td>.889</td>
<td>-.167</td>
<td>-.182</td>
</tr>
<tr>
<td>AS4</td>
<td>361</td>
<td>2</td>
<td>5</td>
<td>3.99</td>
<td>.813</td>
<td>-.364</td>
<td>-.567</td>
</tr>
<tr>
<td>TS1 value</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.57</td>
<td>.790</td>
<td>-.319</td>
<td>.350</td>
</tr>
<tr>
<td>TS2 value</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.58</td>
<td>.782</td>
<td>-.269</td>
<td>.185</td>
</tr>
<tr>
<td>TS3 value</td>
<td>361</td>
<td>2</td>
<td>5</td>
<td>3.83</td>
<td>.758</td>
<td>-.148</td>
<td>-.294</td>
</tr>
<tr>
<td>NS1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>2.83</td>
<td>.915</td>
<td>.128</td>
<td>-.242</td>
</tr>
<tr>
<td>NS2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>2.81</td>
<td>.958</td>
<td>-.061</td>
<td>-.644</td>
</tr>
<tr>
<td>NS3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.01</td>
<td>.877</td>
<td>-.041</td>
<td>-.385</td>
</tr>
<tr>
<td>SmS1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>2.97</td>
<td>.960</td>
<td>-.161</td>
<td>-.432</td>
</tr>
<tr>
<td>SmS2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.71</td>
<td>.891</td>
<td>-.608</td>
<td>.435</td>
</tr>
<tr>
<td>SmS3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.74</td>
<td>.993</td>
<td>-.697</td>
<td>.274</td>
</tr>
<tr>
<td>I1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.48</td>
<td>.847</td>
<td>-.614</td>
<td>.413</td>
</tr>
<tr>
<td>I2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.19</td>
<td>.869</td>
<td>-.125</td>
<td>-.016</td>
</tr>
<tr>
<td>I3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.39</td>
<td>.810</td>
<td>-.235</td>
<td>-.016</td>
</tr>
<tr>
<td>Be1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>2.81</td>
<td>.970</td>
<td>.084</td>
<td>-.582</td>
</tr>
<tr>
<td>Be2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.61</td>
<td>.763</td>
<td>-.393</td>
<td>.250</td>
</tr>
<tr>
<td>Be3</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3.21</td>
<td>.949</td>
<td>-.255</td>
<td>-.365</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>-----</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>C1</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3,81</td>
<td>.752</td>
<td>-.574</td>
<td>.128</td>
</tr>
<tr>
<td>C2</td>
<td>361</td>
<td>1</td>
<td>5</td>
<td>3,83</td>
<td>.711</td>
<td>-.307</td>
<td>.128</td>
</tr>
<tr>
<td>Valid N (listwise)</td>
<td>361</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 3: Cronbach’s alpha.

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS1</td>
<td>10.87</td>
<td>4.169</td>
<td>.699</td>
<td>.531</td>
<td>.711</td>
</tr>
<tr>
<td>AS2</td>
<td>10.95</td>
<td>3.803</td>
<td>.670</td>
<td>.500</td>
<td>.716</td>
</tr>
<tr>
<td>AS3</td>
<td>11.54</td>
<td>4.122</td>
<td>.522</td>
<td>.276</td>
<td>.794</td>
</tr>
<tr>
<td>AS4</td>
<td>10.69</td>
<td>4.227</td>
<td>.571</td>
<td>.349</td>
<td>.766</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>E2</td>
<td>16.69</td>
<td>6.771</td>
<td>.518</td>
<td>.335</td>
<td>.899</td>
</tr>
<tr>
<td>E3</td>
<td>16.20</td>
<td>6.541</td>
<td>.701</td>
<td>.506</td>
<td>.851</td>
</tr>
<tr>
<td>D1</td>
<td>16.24</td>
<td>6.279</td>
<td>.773</td>
<td>.691</td>
<td>.833</td>
</tr>
<tr>
<td>D2</td>
<td>16.25</td>
<td>6.247</td>
<td>.796</td>
<td>.737</td>
<td>.828</td>
</tr>
<tr>
<td>D3</td>
<td>16.19</td>
<td>6.366</td>
<td>.776</td>
<td>.693</td>
<td>.833</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>I1</td>
<td>16.22</td>
<td>9.864</td>
<td>.596</td>
<td>.438</td>
<td>.764</td>
</tr>
<tr>
<td>I2</td>
<td>16.51</td>
<td>9.467</td>
<td>.660</td>
<td>.581</td>
<td>.749</td>
</tr>
<tr>
<td>I3</td>
<td>16.31</td>
<td>9.741</td>
<td>.663</td>
<td>.540</td>
<td>.750</td>
</tr>
<tr>
<td>Be1</td>
<td>16.89</td>
<td>9.506</td>
<td>.553</td>
<td>.309</td>
<td>.775</td>
</tr>
<tr>
<td>Be2</td>
<td>16.09</td>
<td>10.573</td>
<td>.523</td>
<td>.294</td>
<td>.781</td>
</tr>
<tr>
<td>Be3</td>
<td>16.49</td>
<td>10.395</td>
<td>.401</td>
<td>.220</td>
<td>.811</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SmS1</td>
<td>7.45</td>
<td>2.726</td>
<td>.513</td>
<td>.265</td>
<td>.694</td>
</tr>
<tr>
<td>SmS2</td>
<td>6.71</td>
<td>2.735</td>
<td>.591</td>
<td>.353</td>
<td>.605</td>
</tr>
<tr>
<td>SmS3</td>
<td>6.68</td>
<td>2.513</td>
<td>.563</td>
<td>.329</td>
<td>.635</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>U1</td>
<td>8.67</td>
<td>1.495</td>
<td>.588</td>
<td>.352</td>
<td>.560</td>
</tr>
<tr>
<td>U3</td>
<td>8.69</td>
<td>1.491</td>
<td>.530</td>
<td>.305</td>
<td>.624</td>
</tr>
<tr>
<td>U4</td>
<td>9.00</td>
<td>1.400</td>
<td>.485</td>
<td>.241</td>
<td>.689</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Item</th>
<th>Scale Mean if Item Deleted</th>
<th>Scale Variance if Item Deleted</th>
<th>Corrected Item-Total Correlation</th>
<th>Squared Multiple Correlation</th>
<th>Cronbach's Alpha if Item Deleted</th>
</tr>
</thead>
<tbody>
<tr>
<td>TS1 value</td>
<td>7.41</td>
<td>1.802</td>
<td>.684</td>
<td>.534</td>
<td>.685</td>
</tr>
<tr>
<td>TS2 value</td>
<td>7.40</td>
<td>1.758</td>
<td>.728</td>
<td>.565</td>
<td>.636</td>
</tr>
</tbody>
</table>
Appendix 4: Normality PP Plot and Histogram.
Appendix 5: Original multiple regression on the conceptual model

```
. regress Q6Intentionuse FAC1_1 FAC2_1 FAC3_1 FAC4_1 FAC5_1 FAC6_1

Source | SS       df   MS                  Number of obs = 361
--------+--------------------------------------------------
Model   | 138.265872 6    23.044312 F(6, 354) = 28.83
Residual| 282.925264 354  0.799223909 Prob > F = 0.0000
        +--------------------------------------------------
Total   | 421.191136 360  1.16997538 R-squared = 0.3283
        +--------------------------------------------------
          Adj R-squared = 0.3169 Root MSE = 0.89399

Q6Intentionuse | Coef.  Std. Err.     t    P>|t|    [95% Conf. Interval]
-------------+--------------------------------------------------
   FAC1_1      |  0.0534263   0.0537028   0.99  0.320   -.0521903   .159043
   FAC2_1      |  0.1746782   0.0520183   3.36  0.001    0.0723743   0.276982
   FAC3_1      |  0.2021498   0.0506935   3.99  0.000    0.1024516   0.3018481
   FAC4_1      |  0.1165672   0.052055   2.24  0.026    0.0141912   0.2189431
   FAC5_1      |  0.3880994   0.0504965   7.69  0.000    0.2887885   0.4874103
   FAC6_1      |  0.027834    0.0516496   0.54  0.590   -.0737447   0.1294127
    _cons      |  3.811634    0.0470523  81.01  0.000    3.719097    3.904171
```
Appendix 6: Multiple regression with overall security and trust as predictors

```
. regress Q6Intentionuse OverallSecurity OverallTrust

<table>
<thead>
<tr>
<th>Source</th>
<th>SS</th>
<th>df</th>
<th>MS</th>
<th>Number of obs = 361</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model</td>
<td>62.2490231</td>
<td>2</td>
<td>31.1249115</td>
<td>F(2, 358) = 31.04</td>
</tr>
<tr>
<td>Residual</td>
<td>358.941313</td>
<td>358</td>
<td>1.00262936</td>
<td>Prob &gt; F = 0.0000</td>
</tr>
<tr>
<td>Total</td>
<td>421.191136</td>
<td>360</td>
<td>1.16997538</td>
<td>R-squared = 0.1478</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Adj R-squared = 0.1430</td>
</tr>
</tbody>
</table>

| Q6Intentionuse | Coef.   | Std. Err. | t     | P>|t|   | [95% Conf. Interval] |
|----------------|---------|-----------|-------|-------|----------------------|
| OverallSecurity| .2580786| .0723913  | 3.57  | 0.000 | .1157917 .4003656   |
| OverallTrust   | .3342086| .0668521  | 5.00  | 0.000 | .2027363 .4656800   |
| _cons          | 1.683991| .2825545  | 5.96  | 0.000 | 1.128316 2.239666   |
```