NTNU
Norwegian University of
Science and Technology

Master's thesis

2020

Emilie Bjerkelund Stette, Birte Myklebust

Master's thesis

NTNU
Norwegian University of
Science and Technology
Faculty of Economics and Management
Department of International Business

Emilie Bjerkelund Stette
Birte Myklebust

Biometrics used in FinTech

A Technology Acceptance study among Norwegian consumers

July 2020

NTNU
Norwegian University of
Science and Technology

NTNU
Norwegian University of
Science and Technology

Biometrics used in FinTech

A Technology Acceptance study among Norwegian consumers

Emilie Bjerkelund Stette
Birte Myklebust

International Business and Marketing
Submission date: July 2020
Supervisor: Prof. Øivind Strand

Norwegian University of Science and Technology
Department of International Business

Abstract

Purpose - The purpose of this study is to validate the Biometric Technology Acceptance Model proposed by Kanak and Sogukpinar (2017), and to strengthen the model by adding external factors and exploring the effect of trust further.

Theoretical model - The theoretical model used in the thesis is based on the Technology Acceptance Model first introduced by Davis (1989). In this thesis, the TAM model has been extended with trust and external factors (sex, age, experience, and social influence).

Design/methodology/approach - The research questions are answered using a quantitative approach: a questionnaire sent out via Social Media to Norwegian bank customers over the age of 18. The questionnaire is created based on several previous technology acceptance studies. The data gathered from 447 respondents is analyzed using IBM SPSS and SPSS AMOS version 26.

Findings - The main findings are that (1) BioTAM is accepted with a more significant number of respondents, and (2) trust is, by far, the most significant contributor to explaining behavioral intention to use biometric technology in FinTech. Also, perceived usefulness and previous experience with biometric technologies strongly impact the decision to adopt biometrics. This study also highlights the different levels of trust in different market actors, where it is found that traditional banks are most trusted, and FinTech startups are the least trusted. However, trust in startups increases if the startup company enters an alliance with a traditional bank.

Originality/value – Because PSD2 is relatively new, there is limited research on the acceptance of biometrics used in FinTech. This thesis contributes to the technology acceptance literature by confirming the critical role of trust in a consumer's decision to adopt/not adopt. The results also reveal that trust is actor-specific, meaning that the level of trust is dependent on the company offering the biometric technology. It is found that the external factors "sex", "age", and "experience" not only influence perceived usefulness and perceived ease of use, but also has a significant effect on trust. Experience is also found to have a direct effect on intention.

Keywords - technology acceptance, Technology Acceptance Model (TAM), biometrics, trust, social influence, experience, age, Norway

Sammendrag

Formål - Hensikten med denne studien er å validere den foreslåtte biometrisk teknologiske akseptmodellen av Kanak and Sogukpinar (2017) og å styrke modellen ved å legge til eksterne faktorer og utforske effekten av tillit nærmere.

Teoretisk modell – Den teoretiske modellen som er brukt i oppgaven er basert på teknologiaksept modellen som først ble introdusert av Davis (1989). I denne oppgaven er TAM-modellen utvidet med tillit og eksterne faktorer (kjønn, alder, erfaring og sosial påvirkning).

Design/metodologi/tilnærming - Forskningsspørsmålene besvares med en kvantitativ tilnærming: et spørreskjema sendt ut via Sosiale Medier til norske bankkunder over 18 år. Spørreskjemaet er laget basert på flere tidligere teknologiakseptstudier. Data samlet fra 447 respondenter er analysert ved bruk av IBM SPSS og SPSS AMOS versjon 26.

Funn – De viktigste funnene er at (1) BioTAM er akseptert med et større antall respondenter og (2) tillit er den desidert største bidragsyteren til å forklare intensjonen om å bruke biometrisk teknologi i FinTech. I tillegg påvirker faktorer som oppfattet nytte og tidligere erfaringer sterkt beslutningen om å ta i bruk biometri. Denne studien setter også lys på ulike nivåer av tillit til ulike markedsaktører, og det er funnet at tradisjonelle banker har høyest tillit fra forbrukerne og FinTech startups har lavest tillit. Tilliten til startups øker imidlertid dersom de inngår en allianse med en tradisjonell bank.

Originalitet/verdi - Ettersom PSD2 er relativt nytt, er det begrenset med forskning rundt aksept av biometri brukt i FinTech. Denne masteroppgaven bidrar til teknologiaksept-litteraturen ved å bekrefte den viktige rollen tillit har i en forbrukers beslutning om å ta i bruk eller ikke ta i bruk en teknologisk løsning. Resultatene avslører også at tillit er aktør-spesifikk, som betyr at tillitsnivået avhenger av hvilken type aktør som tilbyr løsningen. Det er funnet at de eksterne faktorene «kjønn», «alder» og «erfaring» ikke bare påvirker oppfattet nytte og oppfattet enkelhet, men at de også har en signifikant effekt på tillit. Erfaring har i tillegg en direkte effekt på intensjon om å bruke teknologien.

Nøkkelord - teknologiaksept, Teknologi Aksept Modell (TAM), biometri, tillit, sosial påvirkning, erfaring, alder, Norge

Acknowledgments

This has been a different semester due to the outbreak of Covid-19, but we have been able to complete our thesis thanks to the support of IIF at NTNU.

We would like to thank all the people that have contributed to the result of this thesis:

We would like to express our deepest gratitude to our supervisor, Øivind Strand, for his invaluable support during this semester: for always being available for questions, great input and advice, and for always giving us encouraging words.

We would also like to thank Erik Nesset, for helping us with the analysis and for always being open for questions, and André Schlingloff, for his advice in the initial part of the thesis.

Finally, we would like to thank our families for their support and for sharing our survey with their networks, so that we could have a great starting point for our analyses. Our grateful thanks are also extended to our networks for sharing and participating in our survey.

Table of contents

List of Figures

List of Tables

List of abbreviations

ATT	Attitude
AVE	Average Variance Extracted
BAS	Biometric Authentication System
BI	Behavioral Intention
BioTAM	Biometric Technology Acceptance Model
CB-SEM	Covariance-based Structural Equation Modeling
CER	Crossover Error Rate
EER	Equal Error Rate
FAR	False Acceptance Rate
FinTech	Financial Technology
FRR	False Rejection Rate
IS	Information Systems
PCA	Principal Component Analysis
PEOU	Perceived Ease of Use
PU	Perceived Usefulness
SI	Social Influence
TAM	Technology Acceptance Model
TAM-O	Original TAM
TAM-R	Revised TAM
UTAUT	Unified Theory of Acceptance and Use of Technology
VB-SEM	Variance-based Structural Equation Modeling

Reading guide

Chapter 1 introduces the thesis in general, methods used, and the purpose of the study, including research questions. Contribution and delimitations of the study are also provided in this section.

Chapters 2, 3 & 4 are informative chapters providing the reader with background theory. Chapter 2 provides an overview of the concepts and components used in FinTech. Chapter 3 introduces laws and regulations that developers of biometric technologies are subject to, and chapter 4 gives a review on how biometrics are used in different industries and within the financial sector. The differences in the use of biometrics around the world are briefly discussed.

Chapter 5 gives a presentation of different technology acceptance models, followed by a literature review of previous studies in the field. Then, BioTAM by Kanak and Sogukpinar (2017) is explained in detail. This is followed by an explanation and justification of the extensions made in this thesis.

Chapter 6 explains the choice of data collection method and the development of the questionnaire. Choices and justification of analyses are also included in this chapter.

Chapters 7, 8 & 9 presents the results of this study and discussions. Chapter 7 presents the results of the study and the modifications done to improve model fit. The results of the hypothesis testing are presented in a table at the end of chapter 7. In chapter 8, findings are discussed related to relevant literature. Conclusions are presented in chapter 9.

1 Introduction

The rapid change in the use of technology has forced banks and finance providers to change their way of thinking. This is highly relevant as it will change the way consumers manage their economic errands. There are several studies on technology acceptance, but there is still a literature gap regarding the way customers use and accept biometric payment systems. According to Goode Intelligence, 1.9 billion banking customers will start using biometrics by the end of 2020 (The Future Laboratory, 2019).

The 14th of September 2018, PSD2 was implemented in the EU and EEA, and the Norwegian Ministry of Finance, together with the Norwegian Ministry of Justice, transposed PSD2 into Norwegian Law (Winther, 2019). The Revised Payment Services Directive is believed to completely change the financial environment and allow customers to tailor their banking solution. Understanding people's behavioral intentions towards adopting or rejecting new technology are, therefore, crucial for banks and financial service providers.

Following the implementation of this directive, the banks will be obligated to facilitate the possibility of banking services provided by other actors than the banks themselves. These new third-party actors will heavily increase the competition in the banking sector and force the incumbents to focus on innovation to stay relevant.

The now "old fashioned" card PIN, pocket tokens, and passwords are gradually being replaced by biometrics solutions to reduce cases of fraud and make everyday banking life easier for customers. In Norway, customers have been introduced to biometrics used in payment solutions and other financial technologies through mobile banking apps, Vipps, and Apple/Google Pay, to mention some. These technologies use the fingerprint and facial recognition technologies already incorporated into their smartphones. Vipps has over 100.000 active daily users in Norway as of January 2020 (Stoll, 2020). The technology allows people to interact with payment terminals without physically touching it, and contactless payments such as "tapping", and Apple pay/Google pay are perfect solutions during, for example, the ongoing Covid-19 pandemic.

1.1 Purpose of study

This thesis is based on the study of Kanak and Sogukpinar (2017), where an extension of the Technology Acceptance model is proposed. The new model, called the Biometric Technology Acceptance Model (BioTAM), implements trust as a factor influencing behavioral intention through perceived usefulness and perceived ease of use. BioTAM is tested using a small sample survey to achieve proof-of-concept.

The purpose of this study is to validate BioTAM and to strengthen the model by adding external factors and exploring the effect of trust further. The following research questions will be answered during this thesis:

RQ1: Can BioTAM be validated with a larger sample?

RQ2: Do external factors influence the acceptance of biometric technologies in the financial sector?

1.2 Contribution

During the literature review, it is found that there is a limited amount of research on technology acceptance of biometrics, especially in the context of finance. FinTech startups and incumbent financial institutions will, without a doubt, find great use of a study that explores the factors that affect the consumer's decisions of adoption/no adoption of biometrics. Norway, and the rest of the world, are likely to see an increase in new technologies in the coming years. Awareness of the factors that affect the adoption of these technologies can help developers create relevant products, and to gain a competitive advantage of all the other incumbent and emerging actors in the market. Indirectly, this study will also be beneficial for consumers because the results will help developers create technological solutions that are more relevant to them.

1.3 Research methods

The research questions will be answered using a quantitative approach, with an online survey sent out to Norwegian bank customers from the age of 18, using a convenience sample. The survey is created after a thorough literature review of existing and upcoming biometric technologies, factors that affect the adoption of other financial technologies and biometric technologies in other industries.

Initially, the plan was to implement a mixed-method approach, where the online survey was supplemented with interviews of potential users of the biometric technology. In addition, the plan was to introduce a prototype/mockup of a biometric payment solution to test the reaction of students at the campus. However, these plans were canceled due to the outbreak of Covid-19.

1.4 Delimitations

This study focuses on biometric authentication systems restricted to the financial sector. The research does not take the angle of a specific biometric technology but explores the acceptance of biometrics used in FinTech in general. The reason for this is that advanced biometric technologies are not yet widespread in Norway, and the purpose is to find the factors that affect the adoption of these technologies regardless of what biometric traits are used.

2 Overview of biometrics – concepts and components

In the following section, definitions, and explanations of different concepts relevant to biometric technologies used in FinTech are given.

2.1 Biometrics

Biometrics are referred to as unique identifiable, physiological, or behavioral attributes of an individual (Biometric Institute, n.d.), which can be used for authentication and identification of that individual. Many consumers were introduced to fingerprint authentication when Apple launched iPhone 5S in 2013, and today most smartphone producers use fingerprint recognition (TouchID) or facial recognition (FaceID) (Nyquist, 2019). The Japanese company, NTT DoCoMo, launched its model f505i with a fingerprint sensor as early as in 2003 (Molstad, 2003).

Picture 1: A picture of an iPhone 5S vs the NTT DoCoMo f505i (MyMobileZA, n.d.; NTT DoCoMo, 2003)

2.2 Authentication vs. identification

Biometrics can be used both for identification and authentication. Identification is about correctly determining who a person is (Gemalto, 2020b) based on a 1:n (also called "one to many") comparison (Petersen, 2019). "One to many" comparison means that a biometric trait from a person is compared to that of several other persons in a database (Gemalto, 2020b). In identification, there is no claim of identity (Al-falluji, 2015).

Authentication is about verifying that a person is indeed who (s)he claims to be, based on a 1:1 comparison (Petersen, 2019). "One to one" comparison means that a biometric trait from a person is compared to that registered on the person (s)he claims to be. Biometric authentication is used to verify a person’s identity (Gemalto, 2020b).

2.3 FinTech

FinTech, sometimes referred to as Banking Tech, are “products and companies that employ newly developed digital and online technologies in the banking and financial service industries” (Merriam-Webster, n.d.). FinTech is short for financial technology. The term FinTech is also often used when referring to companies involved in FinTech: startups, incumbent financial firms, and technology companies can all be referred to as FinTechs (PwC, 2016).

Through the world, there is considerable interest in FinTech and disruptive technologies (IKT Norge, n.d.) among startups, BigTechs, incumbent banks, and other financial institutions – and of course, consumers. In the “FinTech ecosystem”, these players are referred to as As, Bs, Cs, and Ds (PwC, 2016).

2.3.1 As – Incumbent financial institutions

As are the established, traditional banks established in Norway. In Norway, the largest banks (measured in the number of customers) are DNB, Nordea, Danske Bank, and the Sparebank 1 alliance (Nestebank, 2020).

2.3.2 Bs - BigTechs

The five big tech companies are Facebook, Amazon, Apple, Microsoft, and Google – abbreviated to FAAMG by Goldman Sachs (Lekkas, n.d). As of January 2020, the five big techs are worth more than $5 trillion together (Winck, 2020). Even though these big tech companies are primarily doing business in other industries, several of them are moving into the financial services industry (Browne, 2020). Not only are they offering payment services, such as Apple Pay and Google Pay, but Apple also launched a credit card in 2019. By the end of 2020, Google will also launch consumer bank accounts (Browne, 2020).

2.3.3 Cs – Companies that provide infrastructure or technology

The Cs are companies that facilitate financial services and transactions for other financial institutions (PwC, 2016). Examples of such companies are MasterCard, Visa, Evry, Nets, and BankID (merged with Vipps and BankAxept in 2018) (BankID, n.d.; Norges Bank, 2020).

2.3.1 Ds – Disruptors / FinTech startups

FinTech startups are newly established companies that offer new technological solutions or existing financial services at a lower cost (PwC, 2016). These startups go directly to the end-user (B2C or B2B) and offer them attractive and innovative solutions, targeting solutions or processes that are neglected by incumbent financial institutions. By developing effective and narrowly defined solutions, these FinTech startups can win customers from traditional banks (Davies *et al.*, 2016).

2.4 Components of biometric authentication systems (BASs)

The technology used in BASs is complex, and there will be no attempt to explain this technology in detail in this thesis. The following is a simple description of the five components used in a typical biometric system. These components are described so that the reader can get a basic understanding of the process that can cause privacy and security concerns among potential users.

The sensor unit is used to collect the biometric data and convert it into a digital format (Gatali *et al.*, 2016). Sensors are important because the entire system depends on the quality of the acquired data and the ability to filter out noise (Kanak and Sogukpinar, 2017; Al-falluji, 2015).

The preprocessing unit is where the biometric data is transformed into a biometric template to be used for matching and verification later (Kanak and Sogukpinar, 2017; Gatali *et al.*, 2016). In this unit, filtering and enhancement techniques are used to remove any excess information and noise, leaving only the data necessary for authentication (Al-falluji, 2015).

The features extraction unit is where the unique characteristics of a person are extracted from the data (Al-falluji, 2015). Examples of such characteristics, using the case of facial recognition, can be the shape of a person’s eyes, nose, mouth, and jaw, also, the distance between these features. Next, the features are encrypted and translated to a password that cannot be reverse-engineered back to an individual (Al-falluji, 2015; Lorvik, 2019). This is referred to as “hashing” or “biohashing”. The point of biohashing is to generate a password, a “binary BioCode”, that represents the biometric data (Belguechi, Cherrier and Rosenberger, 2012).

The data storage component is where the biometric templates from the enrolment process are kept (Gatali *et al.*, 2016).

In *the matching unit*, the stored templates are compared with the newly added data, and the matching algorithm gives an indicator of similarities and dissimilarities between the stored and newly acquired samples (Al-falluji, 2015; Gatali *et al.*, 2016).

Based on the scores from the matching unit, the authentication attempt is either accepted or rejected (Al-falluji, 2015). This fifth component is called the *decision process* and can be both fully automated or human-assisted (Gatali *et al.*, 2016).

2.5 Performance metrics

The performance of a biometric system is rated by different performance metrics, such as “false acceptance rates”, “false rejection rates”, and “equal error rate” (Thakkar, n.d.).

The false rejection rate (FRR), also referred to as type I error, is the probability that the system will reject access to an authorized person. This happens when the system fails to match the input with the already stored template, even though the correct person is attempting authorization (Thakkar, n.d.).

The false acceptance rate (FAR), also referred to as type II error, shows the probability of the system incorrectly authorizing an unauthorized person (Gatali *et al.*, 2016). This can happen when the biometric system matches an input with the already stored template, even though the input is not the same person as in the template (Thakkar, n.d.). False acceptance is usually considered as one of the most severe errors since it means that unauthorized persons gain access to a system that is specifically designed to keep them out (Beal, n.d.).

The equal error rate (EER), also known as the crossover error rate (CER), is the value at which the FRR and the FAR are equal. The EER indicates the performance of the biometric system; the lower the error rate value, the higher the accuracy (Gatali *et al.*, 2016).

2.6 Types of biometrics

There are two main categories of biometrics; physiological measurements and behavioral measurements (Gemalto, 2020b).

Physiological measurements can be divided into biological or morphological. We find measurements such as DNA, blood, urine, or saliva in biological analyses, which is most relevant for the police and medics. For biometrics in FinTech, morphological measurements, such as fingerprints, hand shape, finger shape, iris, facial shape, and vein pattern, are more useful (Gemalto, 2020b).

Behavioral measurements mainly consist of voice recognition, gestures, signature dynamics, keystroke dynamics, gait/sound of steps, and how we use objects (Gemalto, 2020b).

Biometric technologies are continuing to emerge, and measures such as facial thermography, body odor, ear shape, and nailbed identification are some of the exciting technologies that might become relevant in the future (Global Security, 2011).

There have been considerable developments in biometric technologies in recent years. For example, there was a research team at a US University that developed a technique called EarEcho, identifying persons through the geometry of their ear canals (Biometric Technology Today, 2019). Types of biometrics are, therefore, only limited to the imagination and what is “accessible” in terms of a human’s biometrics.

The following is a description of the types of biometrics most used today:

2.6.1 Fingerprint

The patterns on every individual’s fingertips are unique (Global Security, 2011). The fingerprint is one of the most well-known techniques in terms of biometric recognition methods. Darwin’s cousin, Sir Francis Galton, calculated a probability of one to 64 billion in finding two similar fingerprints, even when considering identical twins (Gemalto, 2020b). A live fingerprint reader can scan about 30 specific points (minutiae) in a fingerprint, and evidence by the US FBI state that two individuals cannot have more than eight common minutiae (Gemalto, 2020b).

2.6.2 Facial recognition

This recognition technique requires no physical contact with the persons being identified. This is considered a major benefit as it is non-intrusive, continuous, hands-free, and mostly accepted by users (Global Security, 2011; Gemalto, 2020b). Facial recognition can be done in multiple ways, for example, by using infrared patterns of facial heat emission, or to capture a facial image using an inexpensive camera. Challenges related to facial recognition are to detect masks or photographs (Global Security, 2011).

2.6.3 Voice Recognition

Voice recognition is a technology or program that can decode the human voice. Voice recognition can, for example, be used to interact with a digital assistant such as Google Assistant and Amazon's Alexa. Amazon's Alexa can recognize people by their voice and personalize answers thereafter (Welch, 2017). By using voice recognition systems, a person can perform commands, write, or operate a device without having to touch anything physically (Computer Hope, 2019). Voice recognition software can, for example, be used as an interface with a bank.

2.6.4 Iris Recognition

The iris is the colored area surrounding the pupil of the eye, and these patterns are considered unique for a person. The iris recognition technology has been applied for several years, and the technology works for both identification and verification modes. Iris recognition is more commonly used at border controls to identify travelers as a modality for physical access control. In the past years, it has been implemented into mobile devices for recognition (Findbiometrics, n.d.).

3 Laws and regulations

3.1 GDPR

General Data Protection Regulation within the EU is a legal framework for EU citizens explaining their privacy rights, and at the same time, simplifying companies' requirements when working in several EU countries (Gemalto, 2020a). The primary purpose of the regulation is to have the same legal rules for companies dealing with personal information all over the EU and to enhance the economic growth in these countries (Privacytrust, 2018). The regulation was officially adopted in 2016, and EU-member states had to apply it as of May 2018, replacing any existing national laws. This means that the GDPR law is similar for almost 500 million people. Biometric data is referred to as "special categories of personal data" (Gemalto, 2020a), and the purpose of the law is to protect the EU citizens and residents from having their personal information shared without their consent (Gemalto, 2020a). In Norway, GDPR was adopted on the 20th of July 2018 (Lovdata, 2019).

General data protection rights should be executed at all stages when implementing biometrics in any form in a company (ievo, 2019). GDPR defines biometrics as "personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person" (ievo, 2019, p. 4).

According to the data protection authorities, biometrics are defined as sensitive personal information if there is an intention to identify someone by confirming their identity. The data protection authority also warns about using biometric solutions in situations where it is not necessary to implement in the first place, and that it should not be used unless there is a need for a secure verification (Datatilsynet, 2019).

3.2 PSD2

In the finance sector, PSD2 is highly relevant these days. PSD2 is a new payment service directive that was introduced in January 2018 to regulate the payment systems in Europe. It was applied in Norway on the 14th of September 2019 (Finans Norge, 2019; Finaut, n.d). PwC Norway explains PSD2 as a new era for the financial sector. Two new actors will enter the payment service market: Payment information service provider (PISP) and Account information service provider (AISP). Both have access to withdraw information or provide payment services for customers. This means that FinTech companies can use established banks' infrastructure, such as transaction history and account information, to offer services for their customers. Innovation will be essential to stay competitive in the financial market (Fjørtoft, n.d.; DNB, n.d).

The three primary purposes of PSD2 (Fjørtoft, n.d., p. 4, translated from Norwegian) is to (1) "lead Europe's finance sector to a more integrated and effective payment market", (2) "protect customers by making payments safe and secure", and (3) "create a playground for new payment services (outside of banks) that will increase competition in the market and make it easier for customers to shop for bank services".

PSD2 and biometric authentication go hand in hand. There are strict requirements for customer authentication with PSD2, and using biometrics is a secure way to meet these high requirements (Findbiometrics, 2019).

The PSD2 regulative brings opportunities to other actors in the ecosystem, also banks. Even though the traditional banks are forced to open up their services and products to external actors to stay competitive, opportunities arise as companies can connect through open APIs (Application Programming Interfaces) and together offer the best services for their customers (Guillaume and Horesnyi, 2019).

4 Application of biometrics

4.1 Application in different industries

Biometric technology is evolving at a rapid speed across different industries (Waterson, n.d). This research will mainly focus on the bank and finance sector, but to thoroughly understand the importance and widespread use of biometrics, other industries are therefore briefly discussed.

4.1.1 National identification

In the government sector, biometrics is, for example, used to identify voters, for the safety of the public by using it for criminal identification, and for identifying travelers at cross borders. Many countries have applied these technologies for this purpose (Waterson, n.d).

4.1.2 Healthcare

In the healthcare service sector, biometrics can be used to correctly identify patients and give the right treatment, for example, if a person has been in an accident and is not wearing ID (Waterson, n.d).

4.1.3 Law enforcement

Biometric technologies can be used by law enforcement to identify criminals. For example, live face recognition using surveillance cameras can be used to identify a criminal in a crowd, either in real-time or post-event (Gemalto, 2020b).

4.1.4 Automotive industry

Biometrics ensures that an authorized person is unlocking the doors and starting the car. Inside the car, biometric sensors are scanning the driver's face, iris, voice, or fingerprint to ensure security, comfort, and safety for the driver. For example, physiological measurements such as the heart rate of the driver can be measured in car seats and seatbelts to ensure vehicular safeness by detecting drivers' health and alertness (Aware Inc, 2019).

4.1.5 Other / Covid-19

Covid-19 is forcing banks and other financial institutions to implement biometric identification at a faster speed. The US, for example, has primarily been a cash-based society, while now moving fast to cashless due to the crisis. The virus has shown businesses and people that biometrics can be more hygienic, as well as time and money-saving (Idexbiometrics, 2020; Kawakami, 2020).

4.2 Application of biometrics in banking

The benefits of biometrics, when used in banking, is the protection of information, more secure online banking, fraud protection, and more secure ATM withdrawals (Trader, n.d). Examples of applications in banking are provided below.

4.2.1 Access to accounts

The traditional card PIN, pocket tokens, and password login methods are gradually replaced with biometric technologies to reduce identity theft and fraud. Another benefit is that physical attributes can replace long passwords, making banking easier and more seamless for the customer (Razzak, 2017; Trader, n.d).

4.2.2 ATMs

Biometric authentication in ATMs is at an increasing pace in developed countries. The most suitable biometric technologies for ATM authentication is facial recognition, finger vein pattern, fingerprint, and iris (Trader, n.d). Introducing biometrics to ATM withdrawals has several positive aspects, such as improving customer experience, accuracy, and higher security (Trader, n.d; Razzak, 2017).

4.2.3 Customer service

Fingerprint and facial recognition are already used by Norwegian bank customers to verify their identity before contacting customer service. HSBC in the US, UK, and China is using voice recognition for this purpose. When their customers call customer service, they can say, “my voice is my password” for identification (HSBC, n.d.). In branches, many financial institutions are using finger vein or fingerprint biometrics due to its fast results, as well as being user-friendly and secure before being helped by customer service (Trader, n.d).

4.2.4 Customer onboarding

Refinitiv, a financial sector data provider, launched a digital ID-verification system in 2019, together with Trulioo, a leading global identity and business verification company. The system enables financial institutions to risk-screen and authenticate incoming customers through biometric data to be compliant with KYC (know your customer) and AML (anti-money laundering) regulations. This system conducts anti-impersonation checks, screens for financial and regulatory risks, and other quality checks to help the banks in their combat towards fraud and financial crimes (News in Brief, 2019; Burt, 2019).

4.3 What biometric technologies exist around the world today?

Today we have a “one-size-fits-nobody” digital banking experience, said David Bear, co-founder of 11:FS (The Future Laboratory, 2019). When the number of actors in the financial market increases, the selection from where customers can design and adapt their daily banking expands. It is very likely that every one of us could completely tailor our own banking experience in a few years. Consumers, especially the younger ones, are demanding excellence on all platforms, so banks will need to completely rethink their strategies if they want to stay competitive (The Future Laboratory, 2019).

The following section will briefly look into what biometric technologies exist and are emerging in different parts of the world today. This will indicate what can be expected to see in the financial sectors in the coming years. First, the technology existing around the globe will be examined, with a particular focus on China – the FinTech capital of the world. Next, the technologies that exist and are emerging in Norway will be briefly examined. Due to the rapid growth of biometric technologies around the globe, and the constant change in trends, this will only be an introduction and not a full review of what exists around today.

4.3.1 Biometric technologies around the Globe / China

China is, in many cases, referred to as the FinTech Capital of the world. “If there is a FinTech version of Silicon Valley – it is China. Period” (Sharma, 2016, p. 3). Apps such as Alipay and WeChat give access to services such as payments, investments, loans, social media, travel booking, and credit scores, to mention a few. The Internet giants Baidu, Alibaba, and Tencent (BAT) dominate the FinTech space, and as of 2016, they had about 90% control of the mobile payment market in China (Sharma, 2016).

In China, there is a historic shopping street in Wenzhou City with widespread facial recognition payments (The Future Laboratory, 2019). The government in Wenzhou has entered an agreement with Alibaba and Ant Financial to jointly develop a “smart business area” (China Daily, 2019). The goal is to improve efficiency at peak shopping times and provide a seamless solution for shoppers (The Future Laboratory, 2019). The stores located in Wuma Street have been equipped with Alipay’s system “Dragonfly”, which gives customers the opportunity to go shopping without bringing their wallet or mobile phone, as the payment is made by merely looking at the Alipay device (China Daily, 2019).

The biometric technologies existing in China is simply limited by imagination (Kawakami, 2020). The Chinese will continue to explore and test new and simple ways through biometric technology. It is considered hard, or even impossible, to compete against the FinTech capital of the world.

The differences in how biometric technologies are implemented around the globe today are vast; differences in laws, regulations, and resources are the reason for this.

4.3.2 Biometric technologies in Norway

The DESI (Digital Economy and Society Index) report for 2019 shows that Norway is one of the leading countries in terms of digitalization in the EU, and Norwegian consumers are highly updated in terms of financial technologies today. Norway has large opportunities for growth in FinTech due to its stable financial system (Mortvedt, 2017; European Commission, 2019).

One of the up and coming biometric technologies in the banking sector today is IDEX Biometrics – a biometric smartcard (Biometric technology today, 2018). This is offered by a Norwegian company, using fingerprint identification to ensure simple, personal, and secure authentication when making payments. IDEX Biometrics offers a payment card with a sensor on it, where one identifies oneself just by putting one's finger over the chip (Idexbiometrics, n.d).

Another payment solution that is in the trial phase is a collaboration between DNB and TINE, testing out a facial recognition payment called "Blunk" at a café in Oslo. This technology functions in a way that minimizes the possibility of being subject to fraud because the face-ID is analyzed and transferred into binary codes using biohashing (Giske, 2019).

Vipps, a payment service application introduced by DNB in 2015, is the most popular payment service solution offered in Norway. Vipps had more than 3,2 million users in 2019 (Ghaderi, 2019), and everyone with a Norwegian bank account/card can use Vipps.

Norway is one of the countries that use contactless payments the most, with about 50 percent of all transactions being contactless. However, Norwegian consumers are far behind the other Nordic countries in the use of mobile wallets, such as Apple Pay and Google Pay (Sønsteng, 2020). Only 0.7 percent of Norwegian customers use a mobile wallet, compared to, for example, 7.5 percent in Denmark. In the report made by Adyen, it was found that the average use across the world is close to 5 percent (Sønsteng, 2020). The reason for the low percentage of use in Norway can be that the solutions are not offered by all banks yet – DNB, Norway's largest bank, has, for example, decided not to offer Apple Pay to their customers at this point (Sønsteng, 2020).

5 Factors affecting the adoption of biometric technologies

In the following section, the most common technology acceptance models will be presented before the choice of the model is explained. Technology acceptance models are abundant, such as the Theory of Reasoned Action (TRA) and Theory of Planned Behavior (TPB). However, the most widely used models are the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT). These models have been revised several times. This description includes the basic concepts and constructs behind TAM and UTAUT (Surendran, 2012).

5.1 TAM

The Technology Acceptance Model (TAM), first introduced by Davis (1989), measures perceived usefulness and perceived ease of use to map people's acceptance level to new technology. The model has been used in studies as a framework to explain whether or not people will accept a specific technology and has been extended to several other models, such as TAM 2, TAM 3 (Figure 1) and the Unified Theory of Acceptance and Use of Technology (UTAUT) model (Figure 2) (Kaasbøll, 2009; Surendran, 2012; Boughzala, 2014).

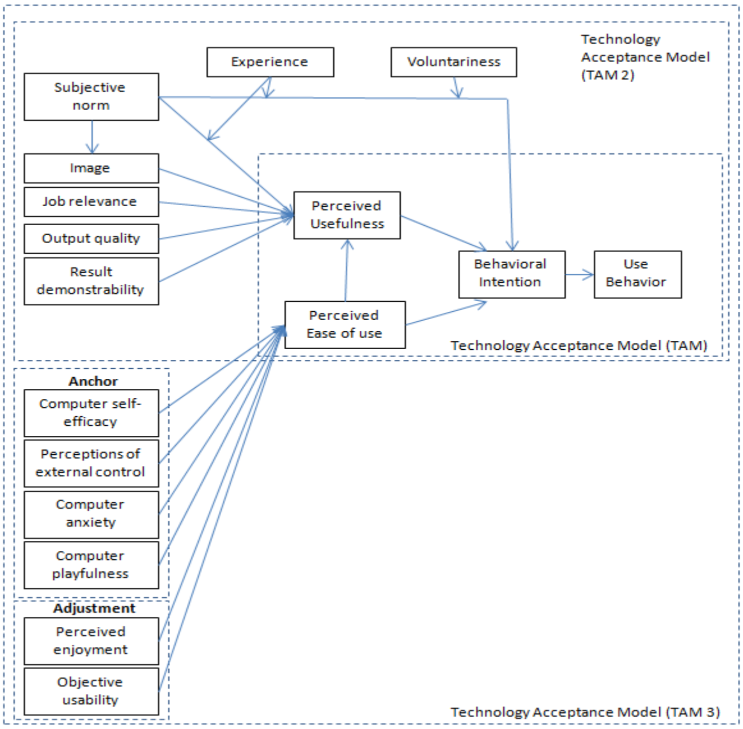


Figure 1 TAM and its extensions (Boughzala, 2014, p. 169)

5.2 UTAUT

Unified Theory of Acceptance and Use of Technology (UTAUT) model measures the likelihood for a person to adopt new technology. UTAUT has emerged from eight different research models; TAM, TRA, TPB, hybrid model TAM-TPB, the model of PC utilization, the motivational model, innovation diffusion theory, and social cognitive theory (Rahi *et al.*, 2019; Boughzala, 2014). As shown in the figure below, facilitating conditions, social influence, effort expectancy, and performance expectancy has a significant influence on behavioral intention to adopt the technology (Rahi *et al.*, 2019).

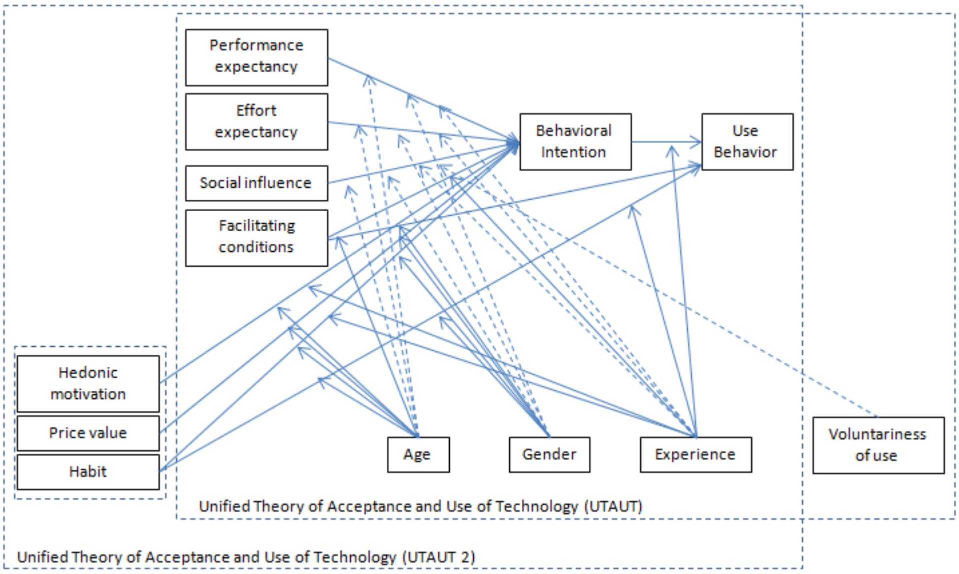


Figure 2 UTAUT and its extension (Boughzala, 2014, p. 170)

5.3 TAM vs. UTAUT – why choose TAM?

Even though there are many technology acceptance models and extensions, the Technology Acceptance Model is the most widely used. The model has been used in several empirical studies and is validated across several fields and situations, which gives TAM high reliability (Boonsiritomachai and Pitchayadejanant, 2017).

In the information systems (IS) research, the TAM model has been used frequently in recent years, although it needs to be extended to strengthen the model (Boonsiritomachai and Pitchayadejanant, 2017; Kanak and Sogukpinar, 2017). According to Kanak and Sogukpinar (2017, p. 458), TAM is used to “better reflect real world challenges”, and it is also a tool to understand customer attitudes and choices with regards to adoption or rejection of technologies (Vahdat *et al.*, 2020).

Several researchers have argued that UTAUT was developed to understand the mandatory use of technologies and might, therefore, have a more limited ability to explain the voluntary use of technologies than TAM (Boonsiritomachai and Pitchayadejanant, 2017). TAM was also initially developed by Davis (1989) to explain technology acceptance in work-related, mandatory settings. However, the model has proven capable of explaining voluntary use – both as it is and through revised/extended models (Morosan, 2011).

Several studies have examined the adoption of novel technologies using different theoretical acceptance models, of which TAM has been considered the most appropriate one (Morosan, 2011). However, TAM has been criticized because it does not sufficiently explain the cognitive processes behind the decision to adopt or not adopt technologies (Kim, Chun and Song, 2009).

There are often many factors involved when predicting human behavior, particularly in the case of sensitive topics such as security and privacy, where the use is voluntary, and the consumers have several different options. It is not possible to cover all factors influencing human behavior, but an extended version of TAM has proven to give a high explanatory power in research (Kanak and Sogukpinar, 2017; Boonsiritomachai and Pitchayadejanant, 2017).

5.4 Literature review

The table below gives a summary of different researchers that have examined the adoption of biometric technologies or other technologies such as internet and mobile banking, the theoretical model used, and their main findings.

Researcher(s)	Research topic	Model	Findings
Miltgen, Popovič and Oliveira (2013)	Determinants of end-user acceptance of biometrics. Uses a scenario method: Access control in a library, using iris recognition	Integration of TAM, UTAUT, and DOI, combined with trust	The results show that Trust is the most important factor explaining Behavioral intention. The acceptance of biometrics is firstly driven by the user's trust in the technology, followed by the user's interest in trying new technologies.

Sharma (2017)	Integrating cognitive antecedents into TAM to explain mobile banking behavioral intention	Extended TAM by incorporating autonomous motivation, controlled motivation, and perceived trust	The R^2 value in the study is higher than in other mobile banking studies. The results show that trust influences users' perceptions of new technology. PEOU and PU influence BI towards mobile banking significantly.
Boonsiritomachai and Pitchayadejanant (2017)	Determinants affecting mobile banking adoption by generation Y based on the UTAUT model, modified by the TAM concept	Integration of TAM and UTAUT2	Facilitating conditions and self-efficacy does not have a direct effect on behavioral intention – nevertheless, they have a positive effect on hedonic motivation. Hedonic motivation serves as a mediator between self-efficacy, behavioral intention, and facilitating conditions. Security has a negative effect on hedonic motivation, and behavioral intention is positively affected by hedonic motivation and self-efficacy.
Chawla and Joshi (2018)	The moderating effect of demographic variables on mobile banking adoption	The constructs from Innovation diffusion theory and TAM models are used	The demographic variables gender, income, age, experience, occupation, qualification, and marital status moderate the impact of independent factors on attitude towards using mobile banking.
Merhi, Hone and Tarhini (2019)	A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers	The UTAUT2 model was modified by adding trust, perceived privacy, and perceived security	Behavioral intention to adopt mobile banking of both countries is influenced by Habit, Perceived Security, Perceived Privacy, and Trust. Performance expectancy and Price value are inversely significant, and Social influence and Hedonic motivation did not reach significance.
Islam *et al.* (2019)	Perception and prediction of intention to use online banking systems	Extended TAM by adding Government Support and Risk	All hypotheses related to PEOU and PU are accepted. Government Support also has a direct effect on Attitude and Risk. The only rejected hypothesis is the relationship between Risk and Intention to use.

5.5 BioTAM

The study by Kanak and Sogukpinar (2017) aims to show how the Biometric Technology Acceptance Model (BioTAM) can be utilized to predict the acceptance of biometric authentication systems (BASs). BioTAM merges the original TAM constructs with the trust model from BioPSTM (Kanak and Sogukpinar, 2014) as a new construct consisting of a privacy-security tradeoff, user confidence, and public willingness. Because they use a small number of respondents, their study gives a “proof of concept” that needs to be validated with a larger sample (Kanak and Sogukpinar, 2017). The constructs of BioTAM (Figure 3) is discussed in detail below:

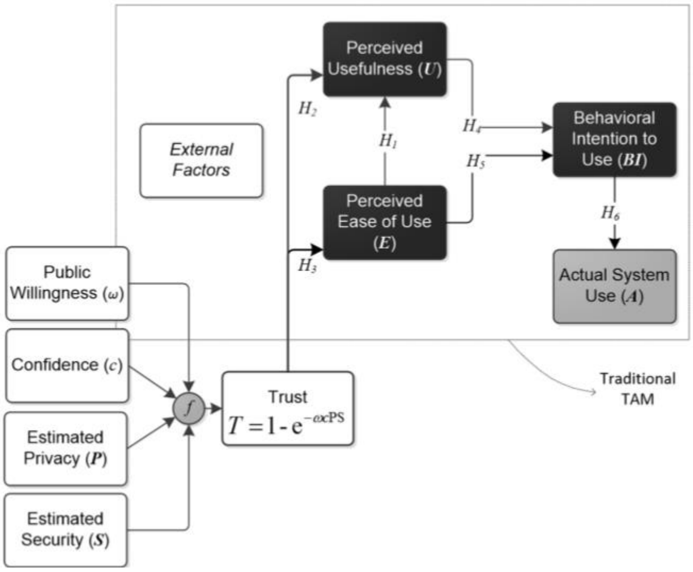


Figure 3 BioTAM (Kanak and Sogukpinar, 2017, p. 459)

5.5.1 Behavioral intention (BI)

Behavioral intention indicates the behavior towards a given technology and is the key concept in the technology acceptance model (TAM) (Sharma, 2017). The concept of behavioral intention can also be found in UTAUT. Earlier research shows that behavioral intention is a major determinant of actual use because people usually consider the implications of using technology before they go through with it (Kanak and Sogukpinar, 2017).

Some studies have included actual use as part of their research (Venkatesh *et al.*, 2003), but most technology acceptance studies have “intention to use” as the dependent variable. In this thesis, the purpose of the model is to determine behavioral intention to use biometric technology among Norwegian bank customers. The framework can subsequently be used to explore factors affecting specific emerging technologies (e.g., payment using facial recognition without having to bring a wallet, phone, or smartwatch).

In BioTAM, the concept of behavioral intention represents the feelings and perceptions towards biometric authentication systems (BASs) (Kanak and Sogukpinar, 2017). In this study, however, the model has been expanded to differ between attitude and behavioral intention.

5.5.2 Perceived usefulness (PU)

Perceived usefulness is explained in the literature as the degree to which a person believes the technological system will improve his or her performance (Lee and Lehto, 2013). Several studies have found that perceived usefulness is the strongest indicator of behavioral intention (Merhi, Hone and Tarhini, 2019).

In BioTAM, the effect of perceived usefulness on behavioral intention is found to be significant, although the R squared is a bit low (.20). This is quite normal in studies predicting human behavior, as these studies usually tend to have R squared values lower than .50 (Frost, n.d.; Kanak and Sogukpinar, 2017). Also, the number of respondents is somewhat low in the BioTAM study (Kanak and Sogukpinar, 2017), as mentioned earlier.

Perceived usefulness is also found in UTAUT, called performance expectancy. It is defined as the “extent of benefit to be had in particular activities due to the use of a technology” (Merhi, Hone and Tarhini, 2019, p. 3).

In this thesis, the effect of perceived usefulness on behavioral intention is tested to confirm the findings of Kanak and Sogukpinar (2017).

5.5.3 Perceived Ease of Use (PEOU)

Perceived ease of use is a concept introduced by Fred Davis (1989, as cited in Merhi, Hone and Tarhini (2019)) in the technology acceptance model and it has since been validated in an extensive number of research projects. PEOU is defined as “the degree to which a person believes that using a BAS would be free from effort” (Kanak and Sogukpinar, 2017, p. 458). It is assumed that users finding technologies easy to use are more likely to adopt these. Several IS researchers have found that PEOU has a significant positive relationship with behavioral intention. The significance of PEOU has been confirmed in Bandura’s (1982, as cited in (Davis, 1989, p. 321) considerable research on self-efficacy, which is defined as “judgments of how well one can execute courses of action required to deal with prospective situations”. More simplified, it means whether an individual believes in hers or his capabilities of using BASs.

In the study of Kanak and Sogukpinar (2017), the relationship between Ease of Use and Trust, and Ease of use and Behavioral Intention had p-values of 0.1 or higher. The researchers suggested an improvement of the questionnaire for the Ease of Use construct. In this thesis, the relationships PEOU to PU and PEOU to BI will be validated with an improved scale, and a higher number of respondents.

5.5.4 Trust

Trust, in this context, is defined as the perception towards the use of technology with regards to security and privacy (Sharma, 2017). A privacy concern means the concern that personal data, such as an individual’s biometric features, are revealed or misused by unauthorized or authorized persons. A security concern means a concern that the system will not recognize a person correctly (Kanak and Sogukpinar, 2017). This is referred to as false positives or false negatives, as discussed earlier in the paper.

Trust is a factor that is highly important for the acceptance of BASs because if compromised, the user cannot change her/his biometric traits the way a stolen password is changed (Biometric Technology Today, 2020).

In a study by Miltgen, Popovič and Oliveira (2013), they propose to combine TAM, UTAUT, and DOI. However, the researchers find that the most important factors to explain the adoption of BASs is not found in these acceptance models, but in the trust literature.

The effect of Trust on Perceived Usefulness and Perceived Ease of Use will be validated.

Kanak and Sogukpinar (2017) use two different measures of trust; one is measured using questions in a questionnaire, and the other is a combination of questions and objective measures. The former consists of two questions, where the respondents are asked to answer on a five-point Likert scale. Of these questions, the researchers make summated scales used for testing the effect of trust on perceived usefulness and perceived ease of use. In addition to testing the hypotheses, Kanak and Sogukpinar (2017) present a trust surface based on the tradeoff between privacy - security, and confidence, and willingness.

5.5.5 Privacy, security, and the tradeoff between them

In BioTam, where the trust surface is based on BioPSTM by the same researchers (Kanak and Sogukpinar, 2014), trust is seen as “an objective measure of privacy-security tradeoff, public willingness and user confidence” (Kanak and Sogukpinar, 2017, p. 457). Kanak and Sogukpinar (2017, p. 457) state that “previous research has shown that a trusted technology is realistic only if the privacy is preserved, security is guaranteed, and confidence in the technology as well as public willingness to adopt the technology are all met”.

Privacy and security are seen as “competing” factors – that is, with increased privacy, the security is degraded and vice versa. The reason is that when biohasing is applied to preserve the privacy of users, the security is reduced because the recognition performance is degraded. The alternate trust construct is set up as a formula showing the level of trust among consumers at an asked privacy and security price (Kanak and Sogukpinar, 2017). Kanak and Sogukpinar (2017, p. 461) state that “if the pareto between privacy (i) and security (ii) is low and users feel confident (iii) and diligent (iv) (public willingness) to use a BAS, one can say that people will most probably trust the BAS”. The trust function is formulated as:

$$T(P,S) = 1 - e^{-wcPS}$$

Where P is privacy, S is security, w is willingness, and c is confidence.

The formula assumes the following:

$$\frac{\partial T}{\partial P} \leq \ 0, \frac{\partial T}{\partial S} \leq \ 0, w > 0, c > 0$$

$$\forall P > 0, \lim_{S \to 0} T(P,S) = 0, \lim_{S \to \infty} T(P,S) = 1$$

$$\forall S > 0, \lim_{P \to 0} T(P,S) = 0, \lim_{P \to \infty} T(P,S) = 1$$

Confidence and willingness are measured using a questionnaire (as with trust, described above), while they use objective measurements of privacy and security. These factors are measured using the performance metrics for the commercial fingerprint authentication system presented to the respondents. Privacy is measured by the average entropy after biohasing is applied, that is, “the average number of trials needed to guess an acceptable binary representation” (Lim and Yuen, 2016, p. 1068). In other words, privacy is measured by the average number of guesses needed to find an accepted binary code representing a biometric template. Security is measured by the Genuine Acceptance Rate (GAR), where FRR is equal to FAR – also known as EER, as discussed in the introduction of this thesis:

$$Security = GAR_{EER} = 1 - EER$$

In this thesis, trust will only be measured using a questionnaire. No trust surface will be made, since this research is about biometric authentication and identification in fintech in general, and not a specific biometric technology, as is the case in the study by Kanak and Sogukpinar (2017). However, this trust surface can be used in further research examining a specific biometric technology, where the average entropy and EER are known.

5.6 Proposed model (model 1)

In this study, an extension of BioTAM, first introduced by Kanak and Sogukpinar (2017), is proposed. The model is extended with the external factors gender, age, experience, and social influence. In addition to validating the original BioTAM model, the effect of these external factors on PU and PEOU is tested. The model has also been extended with attitude, and effects on and of attitude are tested. The figure below shows an overview of the conceptual model and related hypotheses. The constructs marked in blue are from the original BioTAM model, and the constructs and relationships marked in orange are added in this thesis. Further explanation of the choices of hypotheses is provided in the following section.

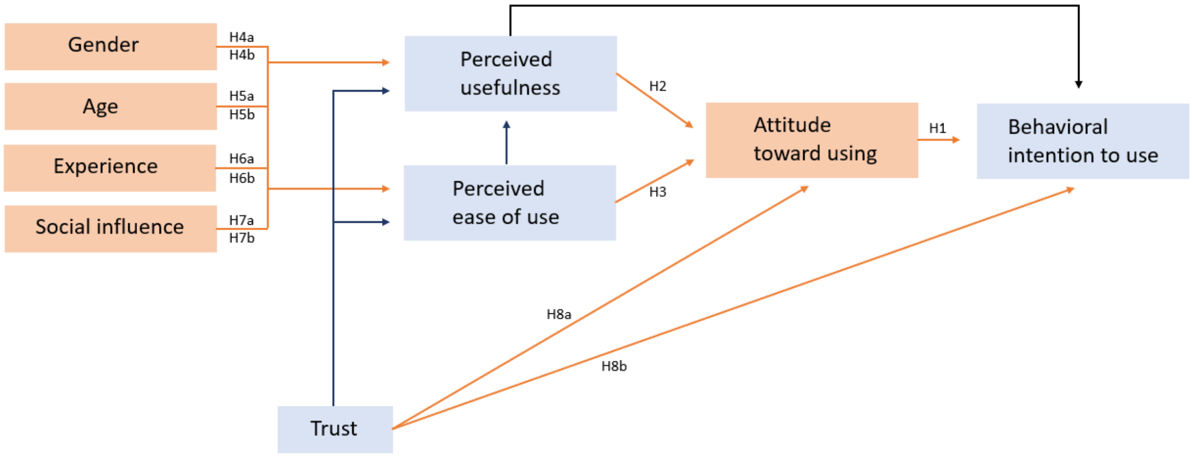


Figure 4 Proposed model and hypotheses

5.6.1 Attitude toward use (ATT)

According to Davis (1989), the attitude construct in TAM measures a person's feelings of favorableness or unfavorableness towards using a specific technology. This is sometimes referred to as "perceived enjoyment" (Boonsiritomachai and Pitchayadejanant, 2017) or "hedonic motivation". Perceived enjoyment, or hedonic motivation, is defined as "the amusement, cheerfulness or pleasure acquired from the use of a technology" (Merhi, Hone and Tarhini, 2019, p. 4).

Perceived enjoyment is found to be an important factor in mobile banking because mobile phones are usually associated with entertainment (Merhi, Hone and Tarhini, 2019). Research conducted in Korea on adopting mobile technologies and services, and mobile banking services, show that attitude is the most significant factor for predicting behavioral intention (Boonsiritomachai and Pitchayadejanant, 2017). Because research shows that attitude has a significant impact on intention to use technology, it is included in recent mobile commerce adoption models (Merhi, Hone and Tarhini, 2019).

There are many theories regarding consumer's attitudes. Hedonic theory (or "theory of psychological hedonism") is a theory of the human response to pain and pleasure. According to the theory, an individual's behavior is motivated by achieving pleasure and avoiding pain or displeasure (iResearchNet, n.d.).

Another theory mentioned in technology adoption research is the valence framework. Valence is the degree of positive or negative feelings toward a particular option (Ogbanufe and Kim, 2018); in this case, the option of using biometric technologies. Ogbanufe and Kim (2018) describes security, usefulness, and convenience as essential elements related to valence.

In the revised version of UTAUT – UTAUT2 – attitude, or hedonic motivation, is added as a construct. However, in revised versions of TAM, attitude is removed from the model. Attitude is treated differently in UTAUT2 and the original TAM. In UTAUT2, hedonic motivation is an independent variable affecting behavioral intention. In TAM, however, attitude is treated as a mediator between ease of use and behavioral intention, and between usefulness and behavioral intention (Boonsiritomachai and Pitchayadejanant, 2017).

Researchers frequently debate the effect of attitude on technology acceptance. When reviewing previous literature, several researchers are in favor of including the construct while just as many are in favor of excluding it. Their opinions on the subject are usually based on the results they have achieved in their research (López-Bonilla and López-Bonilla, 2017; Cheng, Lam and Yeung, 2006).

The TAM model, including attitude, is often referred to as TAM-O (original TAM), whereas the model excluding attitude is referred to as TAM-R (revised TAM) (López-Bonilla and López-Bonilla, 2017). Both models are widely used in technology acceptance studies. López-Bonilla and López-Bonilla (2017) find that the type of analysis can cause different outcomes with regards to acceptance/rejection of the attitude construct. They find that when using VB-SEM, TAM-O is considered the better model, but when using CB-SEM, TAM-R is the better model.

Kim, Chun and Song (2009) believe that the revised TAM model, TAM-R, “underestimates the value of attitude in predicting technology acceptance behavior”, and that using TAM-R in the research of IT acceptance usually bases on empirical findings, but has no theoretical consideration. Because of this, they believe that using TAM-R results in a restricted understanding of the acceptance of technology.

Because the explained variance is low in the original BioTAM model, attitude is included in this thesis to see if it can increase the R squared value and the model fit. The following hypothesis is proposed:

H1: A positive attitude towards biometric technology has a positive effect on behavioral intention.

When attitude is added to the model, the effect of PEOU and PU on attitude must be examined, in addition to the effect of attitude on BI.

5.6.2 Perceived usefulness on attitude

Several studies confirm perceived usefulness' significant impact on attitude; for example, a study done by Islam *et al.* (2019) used attitude as a mediator between PU and intention to use online banking systems. The results of their study are significant, explaining a strong relationship between perceived usefulness and attitude toward use of online banking systems. Another study conducted by Cheng, Lam and Yeung (2006) supports this relationship, as their results show that PU has a significant impact on attitude. The following hypothesis is proposed:

H2: Perceived usefulness has a positive effect on attitude.

5.6.3 Perceived ease of use on attitude

Previous research on perceived ease of use's effect on attitude, such as that of Chawla and Joshi (2018) and Islam *et al.* (2019), shows statistically significant results on the relationship between PEOU and Attitude. Kanak and Sogukpinar (2017) find that the p-values related to hypotheses concerning PEOU are a bit high ($p > 0.1$), both for Trust – PEOU and PEOU – BI. The items making up the PEOU-construct is edited in this thesis to reflect the aspects of ease of use better, as suggested based on the results by Kanak and Sogukpinar (2017). As attitude is included in the proposed extension of BioTAM, the construct will act as a mediator between PEOU and BI, and the effect of PEOU on ATT must be examined. Based on previous research described above, the following hypothesis is proposed:

H3: Perceived ease of use has a positive effect on attitude.

5.6.4 External factors

As noted in the limitations in the study of Kanak and Sogukpinar (2017), the model does not explain all variation in behavioral intention. The researchers suggest that there can be an increased explanatory power and model fit by adding external factors. In this thesis, the external factors included are sex, age, experience, and social influence. The external factors are chosen based on the result of several studies testing the effect of such factors on technology acceptance (Merhi, Hone and Tarhini, 2019; Le *et al.*, 2018), using UTAUT2 and TAM respectively. Sex, age, experience, and social influence are factors found in both versions of UTAUT (Boughzala, 2014). Other studies have also included external factors such as educational background and occupation, but these are not found to be significant in more recent studies (Chawla and Joshi, 2018).

Sex

Previous studies on technology acceptance, using TAM, UTAUT, or a combination of these, show mixed results on the effect of sex. On the one hand, research shows that males are more willing to adopt technology than females in the case of bank technology, Internet banking, and mobile banking (Chawla and Joshi, 2018). Nysveen, Pedersen and Thorbjørnsen (2005, as cited in Chawla and Joshi (2018)) find that males perceive mobile chat services more useful than women, and Zhang, Nyheim and S. Mattila (2014) find that males perceive IS as easier to use than females.

On the other hand, Padilla-Meléndez, del Aguila-Obra and Garrido-Moreno (2013) find no significant differences between men and women, except in the path between PEOU and PU where the coefficient is significantly stronger for males. In addition, Hernández, Jiménez and Martín (2011, as cited in Chawla and Joshi (2018)) find that acceptance, frequency, and satisfaction in relation to the Internet are similar for both genders in Spain.

The findings can be used by FinTech companies and banks to adapt their communication tactics to the different genders if that is found to be significant in this study. The following hypotheses are proposed:

H4a: Sex has a significant effect on perceived usefulness.

H4b: Sex has a significant effect on perceived ease of use.

Age

Research on technology acceptance has shown that age has a strong effect on adoption. There is a consensus in the IS literature that older people are more hesitant to adopt specific technologies (Niehaves and Plattfaut, 2017).

Previous research, such as that of Demirci and Esroy (2008, as cited in Chawla and Joshi (2018)), find that there are more insecurity and discomfort among older people with regards to the use of technology. Younger people tend to be more innovative and are early adopters of new products and services, while older people often have higher technology anxiety (Chawla and Joshi, 2018).

Yi, Wu and Tung (2005, as cited in Chawla and Joshi (2018)) find, in their study of how individual differences influence technology usage, that age has a moderating effect on the relationship between perceptions and use of technology. Fungáčová, Hasan and Weill (2019) find that the level of trust decreases with age.

In the last published annual report by Finans Norge and Kantar TNS from 2018, it is shown that 83 percent of the respondents younger than 32 years are using mobile banking services. In comparison, only 35 percent of respondents over 66 years are using mobile banking. However, there has been a substantial increase; in 2016, only 19 percent of respondents over 66 years were using mobile banking (Finans Norge and Kantar TNS, 2018). The percentage is likely even larger today.

Chung *et al.* (2010, as cited in Niehaves and Plattfaut (2017)) find that there is a negative relationship between age and self-efficacy. There will likely be a visible difference between young and elderly respondents, particularly in the PEOU construct. Therefore, the following hypotheses are proposed:

H5a: Increasing age will have a negative effect on perceived usefulness.

H5b: Increasing age will have a negative effect on perceived ease of use.

Experience

The external factor “experience” is the “familiarity and knowledge about the technology of interest” (Chawla and Joshi, 2018, p. 955). In this thesis, the respondents' experience is the frequency of the use of biometric technologies across industries. This construct is not limited to payment and banking solutions, because the use of the biometric technology will be similar regardless of where it is used for identification and authentication.

Experience is regarded as an important factor in technology acceptance by several researchers, and it is also a factor that is found in both versions of UTAUT. For example, prior experience with similar technology is found to highly influence attitude towards adopting that technology (Alambaigi and Ahangari, 2015). Experience is used as an external factor in technology acceptance studies dating way back, such as that of Irani (2000), where the effect of experience on behavioral intention is found to be significant.

In this thesis, the assumption is that experience of using biometric technology will lead to higher perceived usefulness and higher perceived ease of use. The following hypotheses are proposed:

H6a: Experience has a positive effect on perceived usefulness.

H6b: Experience has a positive effect on perceived ease of use.

Social influence

Social influence means how people are influenced by the opinions of their social network (family and friends). It is defined by Rahi *et al.* (2019, p. 413) as "the extent of social pressure exerted on individuals to adopt new technology".

Even though social influence is a construct used in both versions of UTAUT and extended versions of TAM, the effect of social influence on technology acceptance is highly debated. The effect of social influence is both accepted and rejected in different research. For example, the relationship between social influence and the use of internet banking is found to be significant by Rahi *et al.* (2019), while Gu *et al.* (2009, as cited in Boonsiritomachai and Pitchayadejanant (2017)) find that social influence does not have a significant effect on behavioral intention to use mobile applications. Merhi, Hone and Tarhini (2019) find that there is a difference between countries (Lebanon and England in their case) with regards to the effect of social influence. They find that the effect of SI is stronger in Lebanon than in England.

In this thesis, the effect of social influence on PEOU and PU is examined to see if the relationship is significant in the case of biometric technology in FinTech for Norwegian consumers, with a goal to increase the R squared for BI and to improve model fit. The following hypotheses are proposed:

H7a: Social influence affects perceived usefulness.

H7b: Social influence affects perceived ease of use.

5.6.5 Trust

In the trust-section of BioTAM earlier in this thesis, technology acceptance studies that included trust as a construct are discussed. In BioTAM (Kanak and Sogukpinar, 2017), the effect of trust on perceived ease of use and perceived usefulness is tested. In addition, the direct effect of trust on attitude and behavioral intention is also examined in this thesis.

The effect of "e-trust" on perceived usefulness, perceived ease of use, attitude, and behavioral intention is also examined by (Mansour, 2016), and the effect of e-trust is found to be significant for perceived usefulness, attitude and behavioral intention. Several other researchers also confirm this result: Merhi, Hone and Tarhini (2019) find that trust has a significant positive effect on the intention to use mobile banking for consumers in both England and Lebanon. Alalwan *et al.* (2018) find that trust significantly impacts behavioral intention and perceived usefulness, and Asadi *et al.* (2017) find a significant relationship between trust and behavioral intention.

As mentioned in the literature review, Miltgen, Popovič and Oliveira (2013) find that technology acceptance is primarily explained by trust rather than the traditional technology acceptance constructs. Sharma (2017) finds that trust has a significant effect on perceptions towards technology.

The following hypotheses are proposed:

H8a: Trust has a positive effect on attitude.

H8b: Trust has a positive effect on behavioral intention.

5.6.6 Institutional trust

In Merhi, Hone and Tarhini (2019), trust is found to be an important factor influencing behavioral intention to use technology. They describe two types of trust: institutional trust and trust in technology. Ogbanufe and Kim (2018, p. 5) define institutional trust in the case of e-commerce as "the individual's subjective belief that the online store will fulfill its obligations, as the individual understands them". In their study of fingerprint authentication versus traditional authentication for e-payment, institutional trust is included; however, they discuss trust in an online store as an outcome of the authentication method that the store is using. Ogbanufe and Kim (2018) explain how only a few biometrics studies include trust at all, and those that do, usually only include trust in the biometric technology and its performance, and not trust in the company offering that technology. This is consistent with the findings in the literature review in this thesis; institutional trust is discussed in several studies, but no research examining trust in different actors in the financial market is found in the current review.

Fungáčová, Hasan and Weill (2019) present a cross-country study of trust in banks, where the results show that trust in banks is affected by sociodemographic factors and religious, political, and economic values. Bülbül (2013) examines the factors affecting trust in banking networks (between banks).

Customer perspectives on cloud computing in banking are studied by Asadi *et al.* (2017) using TAM-DTM (diffusion theory model), and the relationship between "trust in vendor" and behavioral intention is found to be significant. Their study does not, however, separate trust in different types of vendors.

A gap exists in the literature regarding institutional trust when it comes to the difference between the level of trust consumers have in different market actors. This is a particularly interesting topic to examine at this time since the financial market will be flooded with different types of actors following the implementation of PSD2.

According to Merhi, Hone and Tarhini (2019), institutional trust can occur because of prior experience with the company or the company's good reputation. This can be hard to apply in a field with novel technology and actors, where the perception of trust rather is influenced by emotional or irrational factors (Merhi, Hone and Tarhini, 2019).

Kanak and Sogukpinar (2017) do not separate between trust in technology and institutional trust in their BioTAM model. This distinction has not been included as a construct in the proposed model either but is examined separately. It is expected that the results will show greater trust in banks than in BigTechs or in unknown fintech startups. However, the trust in non-banks and unknown companies are believed to increase if recommended by a bank.

In a report by PwC (n.d.), together with DNx and Norstat, the trust in technology by Norwegian consumers, is explored. It is found that 68 percent of Norwegian consumers asked, trust Vipps, a service offered by a collaboration of Norwegian banks. On the other hand, only 15 percent trust Apple Pay, offered by the international company Apple. The trust is also low for several other disruptive technologies, such as Bitcoin, Uber, and Foodora.

According to PwC (n.d.), developers depend on customer data to create tailored solutions based on consumer needs; however, the implementation of GDPR has made it more difficult for companies to collect this data without being a highly trusted actor in the market.

6 Methodology / methods

A quantitative approach is selected to test if BioTAM can be validated with a larger sample of respondents and if external factors are influencing acceptance regarding biometrics in the financial sector. A quantitative approach is used in several previous research on TAM (Morosan, 2011; Rahi, Ghani and Alnaser, 2017; Vahdat *et al.*, 2020). BioTAM also uses a quantitative approach by doing a questionnaire (Kanak and Sogukpinar, 2017).

6.1 Data collection and respondents

A convenience sampling is used to recruit respondents for the questionnaire. The questionnaire is published in Social Media (Facebook and LinkedIn) and shared by family and friends. The questionnaire consists of four parts: one part with questions about demographics, one with questions about the respondent's previous knowledge and experience, one part with the constructs from BioTAM, and finally, a part about trust in different actors in the market. The questionnaire is available for respondents online for three weeks.

The questionnaire is directed towards Norwegian bank customers from the age of 18, with no upper age limit. Respondents from the age of 18 are wanted because many under the age of 18 are not responsible for their economy.

The data for the constructs is collected by using statements where the respondents have to answer on a Likert scale from 1 to 7, where 1 means "strongly disagree" and 7 means "strongly agree". All questions in the questionnaire are closed-ended.

Kanak and Sogukpinar (2017) used a 5-point Likert scale in their study, but in this study, a 7-point scale is used. This is based on much reading on the differences between them, without going into details of pros and cons. According to MeasuringU (n.d., p. 2), the short argument is that "having seven points tends to be a good balance between having enough points of discrimination without having to maintain too many response options".

The experience construct is measured by how frequently the respondents use biometric technologies, ranging from "never" to "every day". In this construct, the use of biometrics in general is asked for, not just the use of biometrics concerning banking and payments. This is because the use of biometrics is similar regardless of industry and application, and experience of using it in one application will likely influence their perceptions in other applications.

Throughout the survey, explanations of the different questions are included to ensure that all respondents fully understand the questions asked. This is included based on feedback from the pilot respondents and based on information from previous research. Also, a definition of biometrics is included because previous research shows that consumers know of the technologies but are unfamiliar with the phrase "biometric technologies" (Elliott, Massie and Sutton, 2007).

6.2 Development of questionnaire

The questions for the questionnaire is formulated based on several technology acceptance studies: Kanak and Sogukpinar (2017), Rahi *et al.* (2019), Zhang and Kang (2019), Rahi, Ghani and Alnaser (2017), Boonsiritomachai and Pitchayadejanant (2017), Chawla and Joshi (2018), and Le *et al.* (2018). The questions are translated and formulated in Norwegian to ensure that respondents of all ages understand the questions. Some of the questions included are made specifically for this thesis to strengthen the scales.

For "trust in different actors", all questions are formulated for this thesis because, as discussed in chapter 5.6.6, no research comparing the trust in different actors in the financial market is found in the literature review. The questions in Norwegian, with related references, is found in appendix A. In the text and models, the questions are translated into English.

6.2.1 Pilot survey

Before the questionnaire is published, a pilot test is conducted among 15 colleagues, friends, and family members. They are encouraged to be critical about the layout, language, and interpretation of the questions.

The pilot testers give the following feedback:

- Some questions regarding the use of biometrics lack the option "none".
- The wording in some of the questions: some questions need to be made more specific. For example, the questions that mention biometric technology need to be specified so that the respondents can clearly understand the context of use.
- All questions should have a clarifying explanation, to make it clear what the question is about and make no room for misunderstandings.

6.3 Analysis

Four different analyses are conducted: descriptive analysis, reliability analysis, factor analysis, and SEM/path analysis. A descriptive analysis is conducted to analyze the demographics of respondents and which biometric technologies they have heard of or used before this survey.

6.3.1 Construct reliability

A reliability analysis is conducted to measure the internal consistency of a scale – that is, "the degree to which a set of *indicators* of a *latent variable* is internally consistent based on how highly interrelated the indicators are with each other" (Hair Jr. *et al.*, 2019, p. 609). The purpose of this analysis is to check that the items making up a construct are measuring the same thing (Pallant, 2016). In this thesis, reliability is examined using Cronbach's Alpha value, which is the most used statistic for this purpose. It is recommended that Cronbach's Alpha values are minimum 0.7 (Pallant, 2016; Hair Jr. *et al.*, 2019). The reliability analysis is conducted using IBM SPSS version 26.

6.3.2 Factor analysis

Factor analysis is used as a data reduction technique to reduce the data from a high number of items to a smaller number of constructs without losing information (Hair Jr. *et al.*, 2019). This analysis is also conducted in IBM SPSS version 26, with Principal Component Analysis (PCA) used as the factor extraction method and Direct Oblimin as the method for factor rotation. PCA is commonly used for scale development and evaluation, and Tabachnick and Fidell (2013, as cited in Pallant (2016)) conclude that PCA is the better choice when an empirical summary of the data is wanted. Direct Oblimin is an oblique factor solution, which allows for the factors to be correlated (Pallant, 2016). IBM SPSS only offers exploratory factor analysis, but by forcing the number of components extracted, it is used in this thesis to confirm the predefined constructs.

6.3.3 Construct validity

Two validity measures are used in this thesis: convergent validity and discriminant validity. These are measured in the factor analysis described above.

Convergent validity is assessed using the average mean of squared loadings (AVE) of all items related to a specific construct and show how well the items of the construct converge.

This is often referred to as communality, and the AVE value should be above 0.5 to be acceptable.

Discriminant validity measures the extent to which the constructs are separate from each other (Hair Jr. *et al.*, 2019). This is measured using the Pattern matrix in the factor analysis. The items in a construct should load (strongly) on the same component, and small coefficients under the value 0.5 are therefore suppressed in the analysis.

6.3.4 SEM/path analysis

Structural equation modeling (SEM) is used to examine several interrelated dependence relationships in one analysis simultaneously. The fact that SEM estimates a series of multiple regression equations simultaneously separates it from other multivariate techniques (Hair Jr. *et al.*, 2019). This analysis is conducted using SPSS AMOS version 26, which allows exploring the model as a whole and make changes in the interrelationships if necessary. This is different from the study of Kanak and Sogukpinar (2017), where all hypotheses are analyzed separately. According to Hair Jr. *et al.* (2019, p. 613) "SEM is most appropriate when the researcher has multiple constructs, each represented by several measured variables, and these constructs are distinguished based on whether they are exogenous or endogenous", which is the case in this study.

There are two main types of SEM: variance-based SEM (VB-SEM) and covariance-based SEM (CB-SEM). In this thesis, CB-SEM is used to analyze the data set. This is the classical SEM approach, which has confirmatory characteristics. According to Davcik (2014, p. 23), CB-SEM "is based on the covariance matrices; i.e., this approach tends to explain the relationships between indicators and constructs, and to confirm the theoretical rationale that was specified by a model". This approach is suitable for reflective measurement models with large sample size, examining psychometric factors such as attitudes and intention. This type of SEM also provides universal fit measures (Davcik, 2014). In consultation with the thesis supervisor, generalized least squares (GLS) is chosen as the technique.

In this analysis, the variance in BI explained by the model (R squared), and the contribution of each construct, is examined. The standardized β value is used to examine the contribution of each construct. Using standardized β values allows for comparisons because they have been converted to the same scale (Pallant, 2016). The standardized β value is measured in terms of standard deviations. It shows the standard deviation increase (decrease) in the dependent variable based on a change of one standard deviation in the independent variable (Bhalla, n.d.).

First, the constructs from the original BioTAM model are analyzed, followed by an analysis of the additions and changes made in this thesis.

6.3.5 Model fit

In addition to testing the hypotheses, it is important to examine the model fit of this model. Goodness-of-fit measures indicate how well the theoretical structure specified in the model represents the reality found in the dataset. This is tested by comparing the estimated covariance matrix found in the theoretical model and the actual observed covariance matrix. The two matrices are mathematically compared and can be evaluated through several goodness-of-fit measures (Hair Jr. *et al.*, 2019).

Hair Jr. *et al.* (2019) recommends using at least three to four fit measures to evaluate the model fit adequately. At least one incremental measure and one absolute measure, in addition to the Chi-square ($\chi2$) statistics, should be reported. Based on recommendations from Hair Jr. *et al.* (2019), CFI and RMSEA will be reported in addition to the $\chi2$ statistics.

Chi-square statistics

When applying a Chi-square test to SEM, the null hypothesis is that the observed and estimated covariance matrices are equal, indicating a perfect fit. The $\chi2$ value increases as the differences between the observed and estimated matrix increases, so in SEM, low $\chi2$ values and large p-values indicate a good model fit. The $\chi2$ value is sensitive to large sample sizes and is therefore complemented by other model fit indices Hair Jr. *et al.* (2019).

Absolute fit - Root Mean Square Error of Approximation (RMSEA)

RMSEA is one of the most widely used measures of model fit and is often used in addition to Chi-square because it attempts to correct for large sample sizes and complex models (Hair Jr. *et al.*, 2019). What is considered a good RMSEA value has been debated, but several previous researchers use cut-off values of 0.05 or 0.08. In general, lower RMSEA values indicate better model fit (Hair Jr. *et al.*, 2019).

Incremental fit – Comparative Fit Index (CFI)

Incremental fit measures compare the estimated model to a baseline model. This baseline model assumes that the observed variables are uncorrelated and is often referred to as “null model”. The CFI measure is one of the most widely used incremental fit indices. The value of CFI is ranging from 0 to 1, where higher numbers indicate better model fit (Hair Jr. *et al.*, 2019)

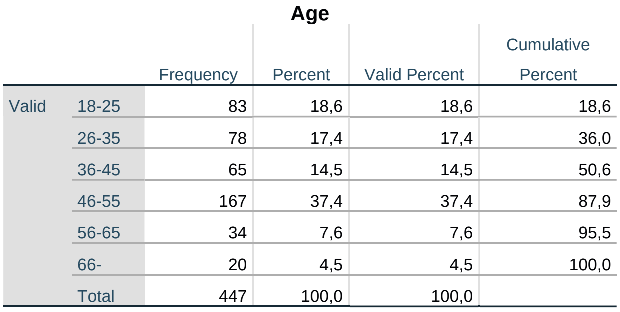
7 Results

All questions were made obligatory, so there are no missing responses in the dataset. In total, 447 responded to the questionnaire.

7.1 Descriptive analysis

7.1.1 Demographics

Of the 447 respondents, 51 percent were male (228), and 49 percent were female (219). Table 1 shows the age distribution of the respondents. As seen in Table 1, there are most respondents in the age group of 46-55, and in the age groups 18-25 and 26-35. The reason is that the survey is distributed in Social Media and shared by friends and family members. Thus, the age of the respondents reflects the age of the network. Still, there are enough respondents in the other age groups as well.



Age

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	18-25	83	18,6	18,6	18,6
	26-35	78	17,4	17,4	36,0
	36-45	65	14,5	14,5	50,6
	46-55	167	37,4	37,4	87,9
	56-65	34	7,6	7,6	95,5
	66-	20	4,5	4,5	100,0
	Total	447	100,0	100,0	

Table 1 Age distribution

7.1.2 Previous knowledge

Of the 447 respondents, 88 percent have heard about biometric technologies before the survey (Figure 5). However, only 2.2 percent answer “none” when asked about which biometric technologies they have heard of prior to the survey. Because of this, it is assumed that the 43 persons that have not heard of biometrics, but then answer that they have heard of a particular technology, are only unfamiliar with the phrase “biometric technologies”.

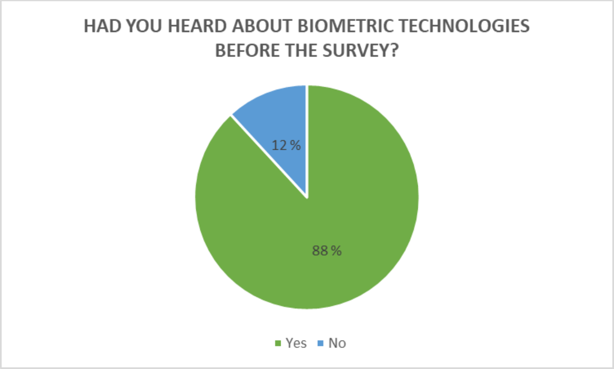


Figure 5 Knowledge of biometrics

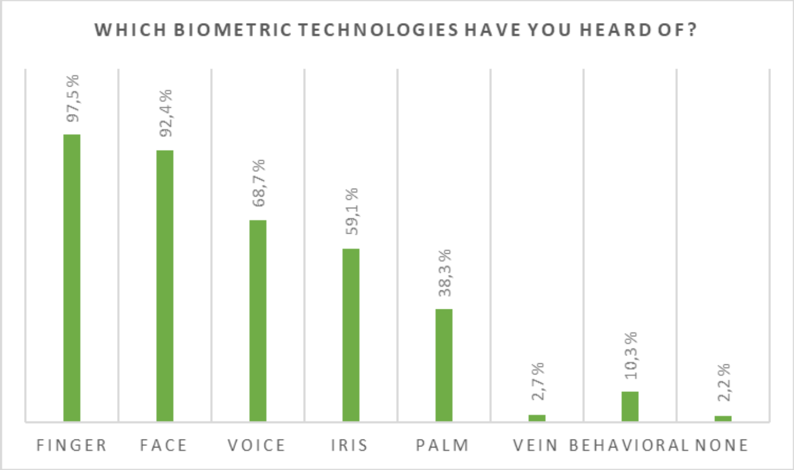


Figure 6 Knowledge of different technologies

Figure 6 shows which biometric technologies the respondents have heard of prior to this survey. Not surprisingly, most respondents have heard of fingerprint recognition (97.5%) and facial recognition (92.4%). In 2018, Statistics Norway found that 95% of the Norwegian population has access to a smartphone, and it is likely that this percentage is even higher in 2020 (SSB, n.d). Most smartphones allow the owner to log in with fingerprint or facial recognition, which can explain why so many have heard of these.

Only a few respondents have heard of the not-so-widespread biometric technologies, such as vein recognition and behavioral biometrics. In this case, the behavioral biometrics asked about is the recognition of how one type or move the computer mouse.

7.1.3 Experience

As mentioned earlier, for the experience construct, the respondents are asked about the frequency of use. Figure 7 shows the percentage distribution of frequency among the respondents. As many as 76.5 percent of the respondents use biometrics (not necessarily related to bank or payments) every day. On the opposite end of the scale, 11.2 percent of the respondents never use biometrics in any context.

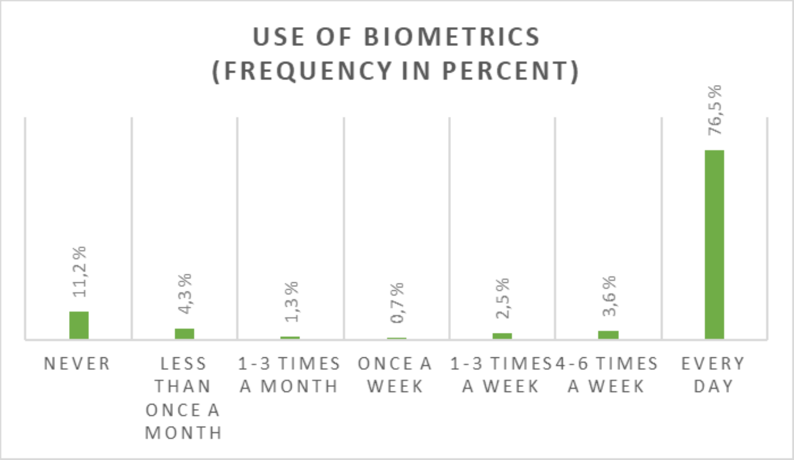


Figure 7 Use of biometrics, frequency

As could be expected, most respondents have used finger (81%) and face technology (53.9%) (Figure 8). Only 8.1 percent of the respondents answer that they have used none of the mentioned biometric technologies. By comparing this number with the number of respondents that have not heard of any biometric technologies, it is found that 26 respondents have heard of, but never used, biometric technologies.

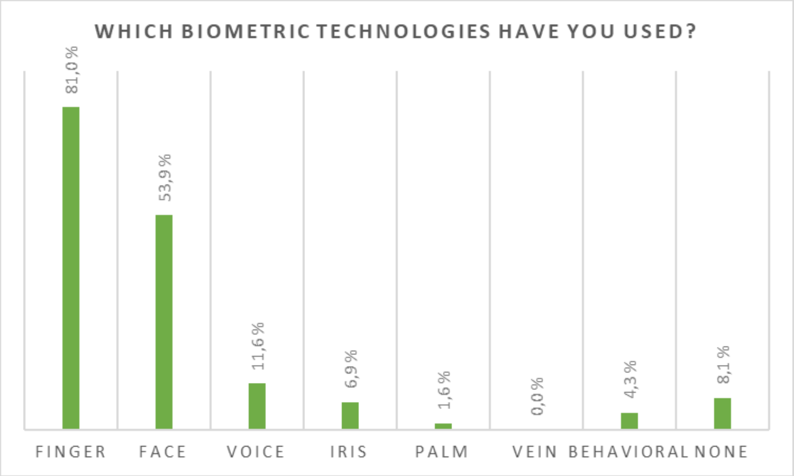


Figure 8 Use of different biometric technologies

7.1.4 Where are biometrics appropriate?

In addition to asking about the respondents' knowledge and experience, it is interesting to find out where they think the application of biometrics is appropriate (figure 9). The respondents are given several different options and can mark all situations where they find biometrics applicable. The situations where biometrics are seen as most appropriate are "logging in to PC/mobile", "Payments in netbank/mobile bank" and "logging in to netbank/mobile bank". Biometrics are already offered as an option to log in to PC/mobile and to log in to mobile banking, so, naturally, people will see these as more appropriate. What is interesting is that "Payments in physical stores" is seen as the third least appropriate. This might have significantly changed these past months, after Covid-19 became a part of everyone's daily life, as all physical contact is avoided – also in stores.

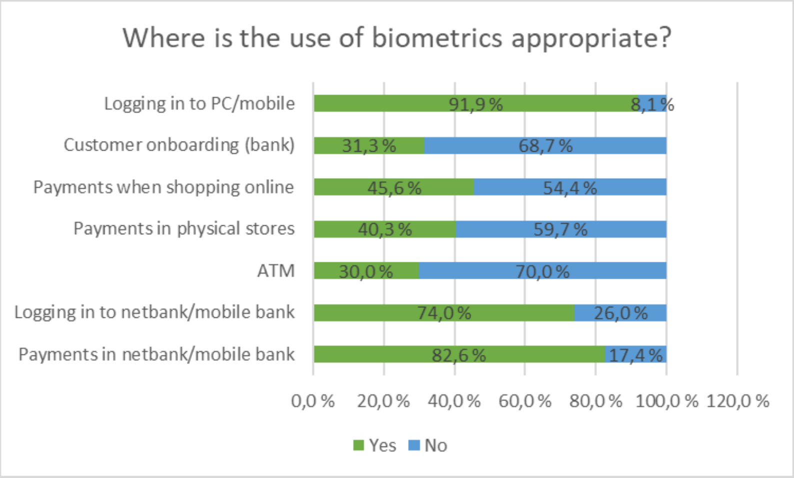


Figure 9 Where biometric technology is appropriate

7.1.5 Assessing Normality

In the descriptive statistics table presented in Appendix B, the questions asked in the questionnaire are represented by mean, St. Deviation, Skewness, and Kurtosis. The distribution of the variables shows negative values for skewness, indicating a clustering on the right-hand side of the graph (appendix C). Two questions have positive skewness: si2 and si4, indicating a clustering on the left-hand side of the graph. The skewness values are ranging from positive 0.453 to negative 2.036, which is a bit too skewed. It should be between 1 and -1, preferably (Smartpls, n.d). Since there exists a substantial amount of skewed data, the distribution is somewhat unsymmetrical (Pallant, 2016).

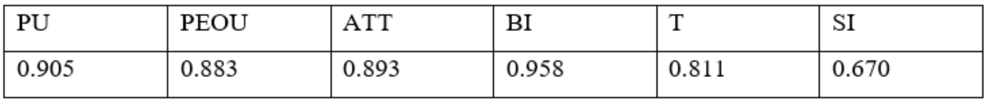
The kurtosis, showing the “peakedness” of the graph, shows mostly positive values, indicating a very centered and peaked graph. Numbers above +1 are too peaked, and numbers less than -1 indicate that the graph is too flat (Smartpls, n.d). There are some kurtosis values higher than 3.00 in the descriptive table (appendix B): for PEOU, all values are above 3, indicating that the variables are non-normally distributed. Both skewness and kurtosis can be affected by large samples (200+), as is the case in this study (Pallant, 2016).

When checking the results of the Kolmogorov-Smirnov test given in the ‘Test of Normality’ tables (appendix D), all values are sig. at 0.000 – which would indicate a violation of normality. This is also normal for larger samples (Pallant, 2016).

None of the variables are removed based on non-normality, but the non-normality is noted. The skewness and kurtosis values are sensitive as the sample size is large. Also, it is expected that people have relatively strong opinions regarding new technology and trust. The results can, therefore, be assumed to be in the extreme, and non-normality can be expected.

7.2 Reliability analysis

Table 2 shows the Cronbach’s Alpha value for each of the constructs, with all items included (tables from SPSS included in appendix E-J):



PU	PEOU	ATT	BI	T	SI
0.905	0.883	0.893	0.958	0.811	0.670

Table 2 Cronbach's Alpha values for the constructs

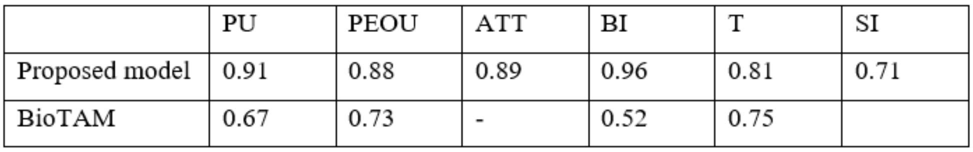
For Social Influence, Cronbach’s Alpha is below 0.7. This indicates that one or more of the items should be removed. In the Item-Total Statistics, the “Cronbach’s Alpha if item deleted” column (appendix J) shows that the Alpha value will be 0.707 if item 1 is removed.

Running a new reliability analysis without item 1 (appendix K) gives correlations above .3 (although they are still a bit low). This second analysis shows that the Alpha value will be increased to 0.714 if item 3 is removed as well.

The results of the reliability analysis show that all the scales have good internal consistency and that they measure the same underlying characteristics (Pallant, 2016). The Alpha value for SI is increased to 0.714 by removing items 1 and 3, which suggests that these should be considered removed from the scale.

Hair Jr. *et al.* (2019) argue that Cronbach’s Alpha values between 0.70 and 0.95 are “acceptable to good”, while any values above 0.95 are considered too high and unrealistic. Other literature argues that 0.90 is too high (Tavakol and Dennick, 2011), and some say ‘the higher, the better’ (Statistics Solutions, n.d). According to Hair Jr. *et al.* (2019), the alpha value of BI (0.958) is slightly too high. The reason behind this can be that the questions are too similar, causing redundancy. When checking the “Cronbach’s Alpha value if item deleted” (appendix H), removing one of the items only has a small effect on the alpha value, and all items are therefore kept.

In the study of Kanak and Sogukpinar (2017), the researchers report that scales with a Cronbach’s Alpha coefficient above 0.5 are sufficiently reliable. In this study, all Cronbach’s Alpha values are increased compared to the constructs used in BioTAM. Table 3 shows a comparison between the Cronbach’s Alpha values in this study and the values found by Kanak and Sogukpinar.



	PU	PEOU	ATT	BI	T	SI
Proposed model	0.91	0.88	0.89	0.96	0.81	0.71
BioTAM	0.67	0.73	-	0.52	0.75	

Table 3 Comparison of Cronbach’s Alpha values

7.3 Factor analysis

After confirming internal consistency in the reliability analysis, the next step is to conduct a factor analysis using SPSS to reduce the data into constructs. Since the number of constructs is already predetermined, a forced five-factor solution is computed. The goal is to confirm that the items in each of the constructs are loading on the same factor.

To be suitable for factor analysis, it is important to have a sufficient sample size. Tabachnick and Fidell (2013, as cited in Pallant (2016)) suggest that there should be at least 300 cases when conducting a factor analysis. Nunnally (1978, as cited in Pallant (2016)) suggests a 10 to 1 ratio – that is, ten cases to each item. In this case, there are 20 items included. With 447 respondents, both criteria above are fulfilled.

7.3.1 Factor analysis including all items

First, a factor analysis with all items included for PU, PEOU, ATT, BI, and SI is conducted. The Correlation Matrix (appendix L) shows several correlations above 0.3, which is required for the factor analysis to be suitable. The Kaiser-Meyer-Olkin (appendix M) measure of sampling adequacy is 0.929, which is higher than the recommended value of minimum 0.6 (Pallant, 2016). Bartlett's Test of Sphericity reaches statistical significance ($p < 0.001$).

Because the goal of this factor analysis is to confirm the loadings on each construct, there is no need to determine the number of factors to extract using Kaiser's criterion or the Scree plot. The number of factors to extract has been predetermined by forcing a five-factor solution, as mentioned above. The "Total Variance Explained" table shows that five factors are explaining 77.5% of the variance (Appendix N).

In the Communalities table (appendix O), all the values are relatively high, above 0.3, as suggested in Pallant (2016). The two lowest values in this table are items 1 and 3 in SI (0.455 and 0.605, respectively). These values were suggested for removal in the reliability analysis, and the findings in the Communalities table support that.

Oblimin rotation provides a Pattern Matrix (appendix P), where the factor loadings on each of the components are displayed. Only loadings higher than 0.5 will be included in the constructs in this thesis, and SPSS is therefore set to suppress loadings of 0.5 and lower. Three items do not have loadings above 0.5 and will, therefore, not be used in the constructs. These three items are Si1, Si3, and Att1.

7.3.2 Running a new factor analysis without Si1, Si3, and Att1 (appendix Q-S)

In the Communalities table, all values are now above 0.7. The variance explained has increased to 82.3%. In the Pattern Matrix, all items are loading on the correct component, corresponding with their construct.

7.3.3 Including trust to confirm that it is loading as a separate component (appendix T-U)

With a forced six-factor solution including the Trust-construct, the Pattern Matrix show all items loading on the correct component, and all values are above 0.5, indicating good discriminant validity. All AVE values in the Communalities table are above 0.7, above the minimum accepted value of 0.5, which indicates a good convergent validity. Therefore, the following summated scales will be computed:

Perceived usefulness

PU1: Biometric technology will make me pay faster

PU2: Biometric technology will make it easier for me to do bank errands

PU3: Biometric technology will increase my productivity

PU4: Biometric technology is useful for me in banking

Perceived ease of use

PEOU1: Biometric technology is easy to use

PEOU2: Biometric technology is easy to learn

PEOU3: Biometric technology is easier to use than other solutions

PEOU4: I can learn to use biometric technology without help

Attitude

ATT2: Biometrics give me a positive experience

ATT3: Using biometrics is fun

ATT4: Using biometrics is exiting

Behavioral intention

BI1: I will use biometric technology in banking and payment context

BI2: I will use biometrics on a regular basis

BI3: I will choose biometrics over other methods

BI4: I will use the biometric technologies that exist

Social influence

SI2: I am influenced by my social circle to use biometrics

SI4: Using biometrics gives me status in my social circle

Trust

T1: I trust biometric technology more than other solutions

T2: I trust biometric technology to identify me correctly

7.3.4 Summary of validity and reliability measures

Constructs and items	Communalities	Factor loading	Cronbach's Alpha
PU			0.905
- pu1	0.806	0.771	
- pu2	0.890	0.880	
- pu3	0.794	0.689	
- pu4	0.808	0.529	
PEOU			0.883
- peou1	0.808	0.895	
- peou2	0.821	0.892	
- peou3	0.703	0.616	
- peou4	0.728	0.838	
ATT			0.893
- att2	0.777	0.565	
- att3	0.875	0.891	
- att4	0.883	0.934	
BI			0.958
- bi1	0.920	0.910	
- bi2	0.918	0.926	
- bi3	0.833	0.735	
- bi4	0.896	0.825	
SI			0.714
- si2	0.784	0.892	
- si4	0.776	0.872	
T			0.811
- t1	0.857	0.915	
- t2	0.823	0.839	

7.4 SEM / path analysis

The computed constructs above are used to test the hypotheses, in addition to the external factors age, sex, and experience. Age, sex, and experience only consist of one question from the questionnaire, so no new variables need to be computed. The external variables sex, age, and experience are coded in SPSS in the following way:

Sex is coded as a dummy variable, where female responses are coded as 0, and male responses are coded 1. No respondents answered “other”, so this option is not coded. For age, six different age groups are used. The age groups are recoded into a scale from 1 to 6: 1 = 18-25, 2 = 26-35, 3 = 36-45, 4 = 46-55, 5 = 56-65, 6 = 66+. Experience consists of seven different frequencies of use. These frequencies are coded from 1 to 7, where 1 is never, and 7 is every day.

First, the original BioTAM model is validated with a larger sample, and next, the additional hypotheses included in this thesis are tested.

7.4.1 Validation of BioTAM

One significant difference between the analysis of the hypotheses in BioTAM and the hypotheses in this thesis is that Kanak and Sogukpinar (2017), from the information given in their research, appear to have analyzed one by one hypothesis independently and receive an R squared value for each of the hypothesis. In this thesis, all hypothesis will be put into the same model to get the total effects of all constructs. This can have an impact on the ability to compare the R squared values achieved in this thesis with the ones found by Kanak and Sogukpinar (2017). All hypotheses made by Kanak and Sogukpinar (2017), except the hypothesis regarding actual use, were subject to validation in this thesis.

In the original BioTAM model, the R squared values were quite low, ranging from <0.00 to 0.20. With a more significant number of respondents and improvement of the questionnaire, it is found that the R squared value for Behavioral intention (figure 10) is 0.69 in this thesis, which is a good result in a study of human behavior (Kanak and Sogukpinar, 2017).

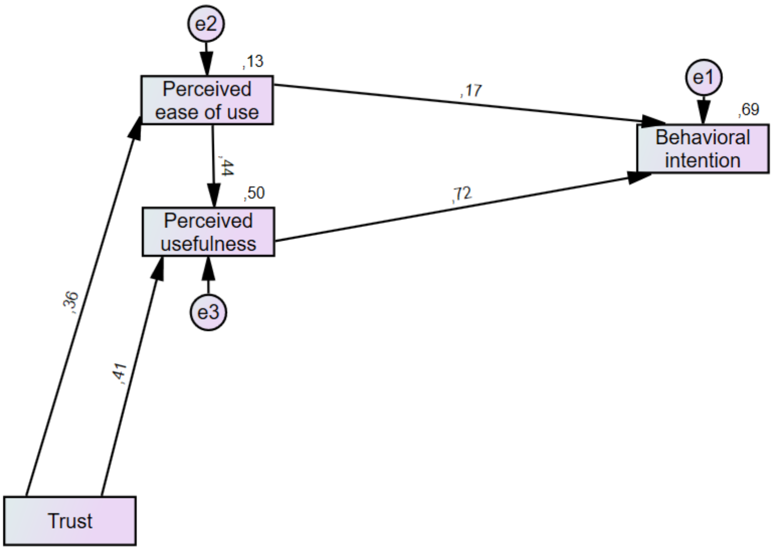
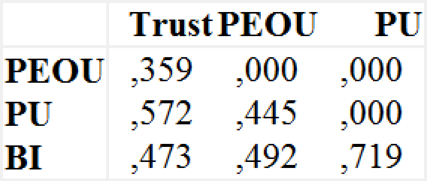


Figure 10 BioTAM with R squared and standardized regression weights

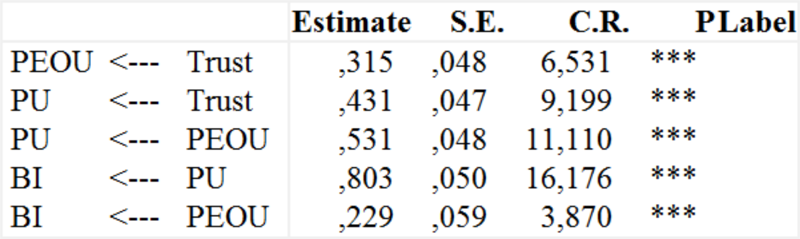
It is found that Trust has a large impact on both PU and PEOU, with β values of 0.41 and 0.36 (Figure 10). Looking at standardized total effects (Table 4), PU has the largest total effect on BI, followed by PEOU and then Trust. This conflicts with recent studies, where the results show that Trust has a larger effect on the intention to use technology than traditional technology acceptance constructs (Miltgen, Popovič and Oliveira, 2013).



	Trust	PEOU	PU
PEOU	,359	,000	,000
PU	,572	,445	,000
BI	,473	,492	,719

Table 4 BioTAM: Standardized total effects

All hypotheses are significant, with p-values lower than 0.001(Table 5). In the study conducted by Kanak and Sogukpinar (2017), p-values are ranging from 0.01 to 0.56. Two of their hypotheses are not accepted at p-value 0.5: “high trust on a BAS will lead to increased perceived usefulness” and “behavioral intention of users to use a BAS positively influences the actual usage”.

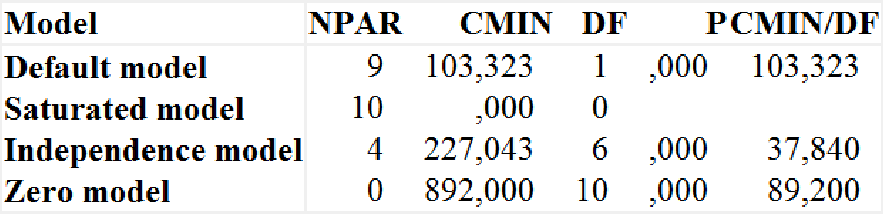


			Estimate	S.E.	C.R.	P	Label
PEOU	<---	Trust	,315	,048	6,531	***	
PU	<---	Trust	,431	,047	9,199	***	
PU	<---	PEOU	,531	,048	11,110	***	
BI	<---	PU	,803	,050	16,176	***	
BI	<---	PEOU	,229	,059	3,870	***	

Table 5 BioTAM: p-values

Model fit

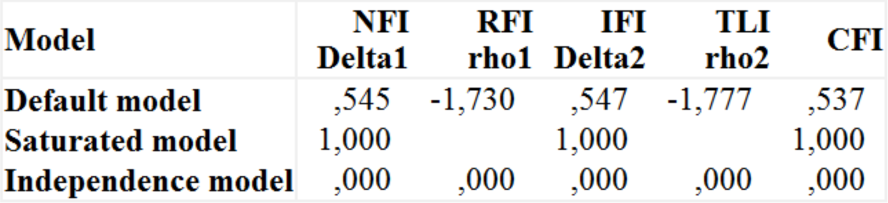
For this model, the χ^2 value is 103.323, with 1 degree of freedom (Table 6). The p-value is less than 0.01, which means that there is a significant difference between the observed and estimated covariance matrices. This indicates a poor model fit. However, with a high number of respondents, it is harder to achieve an insignificant χ^2.



Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	9	103,323	1	,000	103,323
Saturated model	10	,000	0		
Independence model	4	227,043	6	,000	37,840
Zero model	0	892,000	10	,000	89,200

Table 6 BioTAM: Chi-square statistics

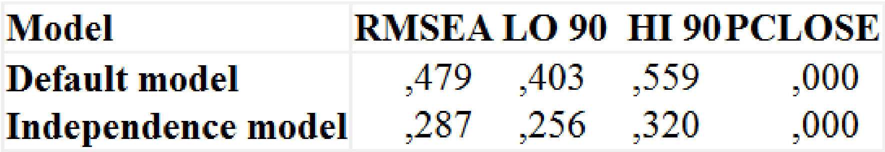
The CFI value is 0.537, which is also indicating a poor model fit (Table 7). Preferably, the CFI value should be as high as possible and at least higher than 0.90 (Hair Jr. *et al.*, 2019; Parry, n.d.).



Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,545	-1,730	,547	-1,777	,537
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

Table 7 BioTAM: CFI

The RMSEA value should be as low as possible and at least lower than 0.08. For this model, the RMSEA value is 0.479 (Table 8). Based on the three measures of model fit used in this thesis, the model has a poor fit.



Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,479	,403	,559	,000
Independence model	,287	,256	,320	,000

Table 8 BioTAM: RMSEA

7.4.2 Proposed model – model 1

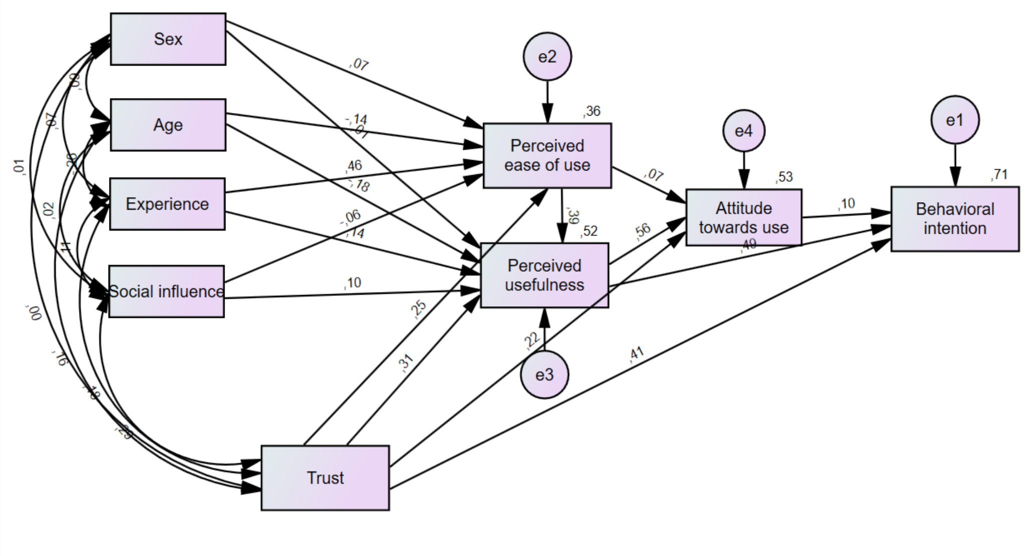
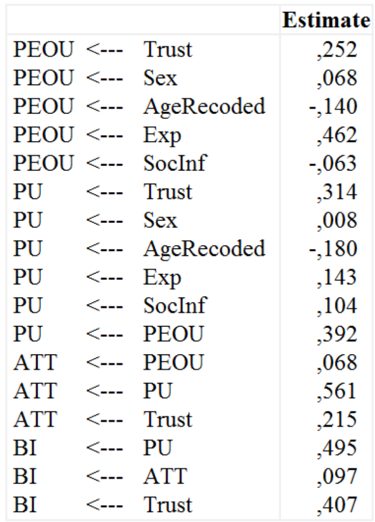


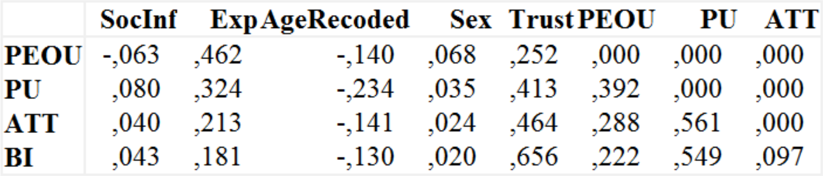
Figure 11 Proposed model

In the proposed model, the results show that the R squared have increased slightly, to 0.71 for BI (figure 11). This means that this model better explains the variance in behavioral intention (Pallant, 2016).



			Estimate
PEOU	<---	Trust	,252
PEOU	<---	Sex	,068
PEOU	<---	AgeRecoded	-,140
PEOU	<---	Exp	,462
PEOU	<---	SocInf	-,063
PU	<---	Trust	,314
PU	<---	Sex	,008
PU	<---	AgeRecoded	-,180
PU	<---	Exp	,143
PU	<---	SocInf	,104
PU	<---	PEOU	,392
ATT	<---	PEOU	,068
ATT	<---	PU	,561
ATT	<---	Trust	,215
BI	<---	PU	,495
BI	<---	ATT	,097
BI	<---	Trust	,407

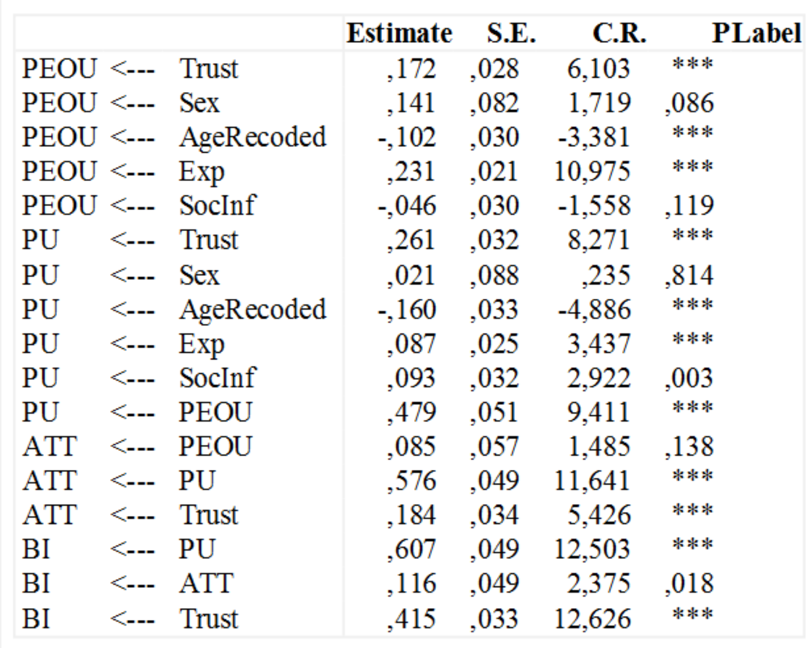
Table 9 Standardized regression weights



	SocInf	Exp	AgeRecoded	Sex	Trust	PEOU	PU	ATT
PEOU	-,063	,462	-,140	,068	,252	,000	,000	,000
PU	,080	,324	-,234	,035	,413	,392	,000	,000
ATT	,040	,213	-,141	,024	,464	,288	,561	,000
BI	,043	,181	-,130	,020	,656	,222	,549	,097

Table 10 Standardized total effects

The largest direct effects are found by looking at the standardized β values (table 9). For this model, the results show that PU to ATT, PU to BI, Experience to PEOU, and Trust to BI have the largest values. The standardized total effects (table 10) show that Trust has the largest effect on BI, followed by PU. Also, the standardized total effects show that Sex, Social Influence, and Attitude has the smallest effect on BI.



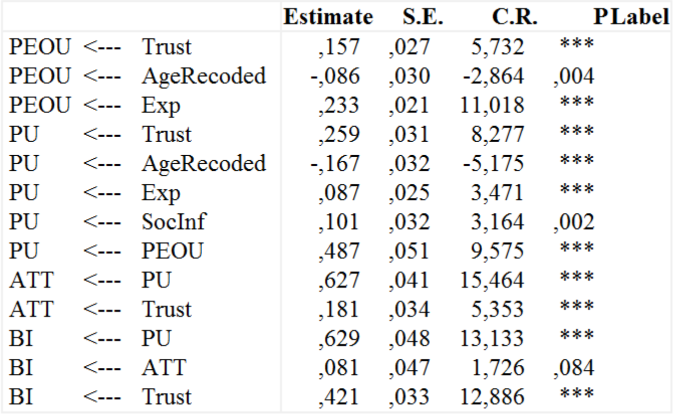
			Estimate	S.E.	C.R.	P	Label
PEOU	<---	Trust	,172	,028	6,103	***	
PEOU	<---	Sex	,141	,082	1,719	,086	
PEOU	<---	AgeRecoded	-,102	,030	-3,381	***	
PEOU	<---	Exp	,231	,021	10,975	***	
PEOU	<---	SocInf	-,046	,030	-1,558	,119	
PU	<---	Trust	,261	,032	8,271	***	
PU	<---	Sex	,021	,088	,235	,814	
PU	<---	AgeRecoded	-,160	,033	-4,886	***	
PU	<---	Exp	,087	,025	3,437	***	
PU	<---	SocInf	,093	,032	2,922	,003	
PU	<---	PEOU	,479	,051	9,411	***	
ATT	<---	PEOU	,085	,057	1,485	,138	
ATT	<---	PU	,576	,049	11,641	***	
ATT	<---	Trust	,184	,034	5,426	***	
BI	<---	PU	,607	,049	12,503	***	
BI	<---	ATT	,116	,049	2,375	,018	
BI	<---	Trust	,415	,033	12,626	***	

Table 11 Proposed model: p-values

Table 11 shows that the effect of Sex on PU and PEOU is not significant (H4a and H4b). This is also the case for the effect of SI on PEOU (H7b) and the effect of PEOU on ATT (H3). The effect of SI on PU (H7a) is statistically significant at $p < 0.01$, and the effect of ATT on BI (H1) is significant at $p < 0.05$. H2, H5a, H5b, H6a, H6b, H8a, and H8b are statistically significant, with p-values < 0.001.

Based on this, H3, H4a, H4b, and H7b are rejected and removed from the model.

7.4.3 Model 2: Removing Sex, PEOU on ATT, and SI on PEOU



			Estimate	S.E.	C.R.	P	Label
PEOU	<---	Trust	,157	,027	5,732	***	
PEOU	<---	AgeRecoded	-,086	,030	-2,864	,004	
PEOU	<---	Exp	,233	,021	11,018	***	
PU	<---	Trust	,259	,031	8,277	***	
PU	<---	AgeRecoded	-,167	,032	-5,175	***	
PU	<---	Exp	,087	,025	3,471	***	
PU	<---	SocInf	,101	,032	3,164	,002	
PU	<---	PEOU	,487	,051	9,575	***	
ATT	<---	PU	,627	,041	15,464	***	
ATT	<---	Trust	,181	,034	5,353	***	
BI	<---	PU	,629	,048	13,133	***	
BI	<---	ATT	,081	,047	1,726	,084	
BI	<---	Trust	,421	,033	12,886	***	

Table 12 p-values

After removing the insignificant hypotheses, the results show that the effect of ATT on BI is also insignificant and has a very low standardized β value (0.068) (Table 12). The results show that Trust and PU has a significant effect on ATT, but there is no significant effect of ATT on BI. Since the goal of this study is to determine factors affecting behavioral intention to use biometric technologies, it is decided that attitude be removed from the model.

7.4.4 Model 3: Removing ATT and adding a link between PEOU and BI

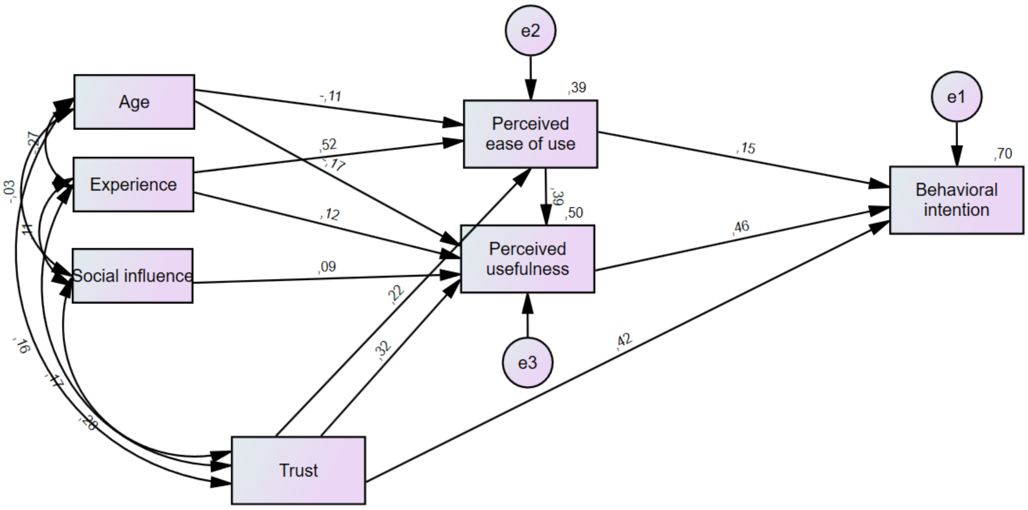
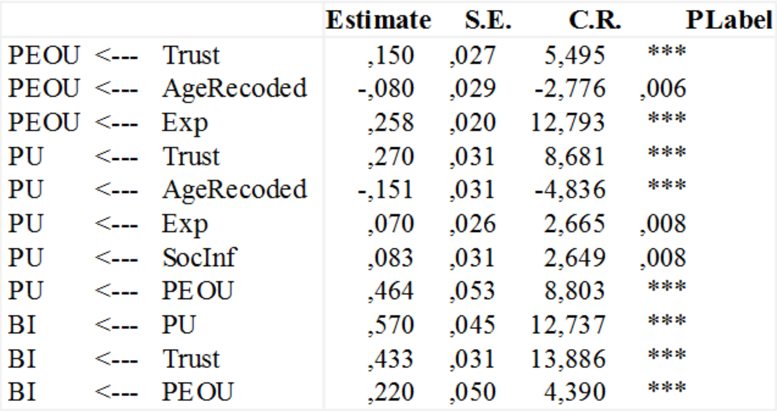


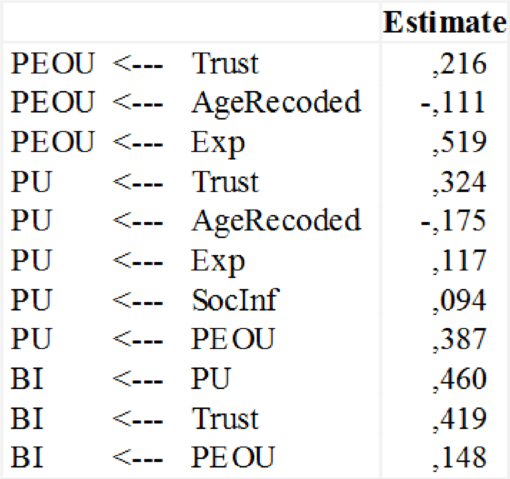
Figure 12 Proposed model after removing insignificant links



			Estimate	S.E.	C.R.	P	Label
PEOU	<---	Trust	,150	,027	5,495	***	
PEOU	<---	AgeRecoded	-,080	,029	-2,776	,006	
PEOU	<---	Exp	,258	,020	12,793	***	
PU	<---	Trust	,270	,031	8,681	***	
PU	<---	AgeRecoded	-,151	,031	-4,836	***	
PU	<---	Exp	,070	,026	2,665	,008	
PU	<---	SocInf	,083	,031	2,649	,008	
PU	<---	PEOU	,464	,053	8,803	***	
BI	<---	PU	,570	,045	12,737	***	
BI	<---	Trust	,433	,031	13,886	***	
BI	<---	PEOU	,220	,050	4,390	***	

Table 13 p-values

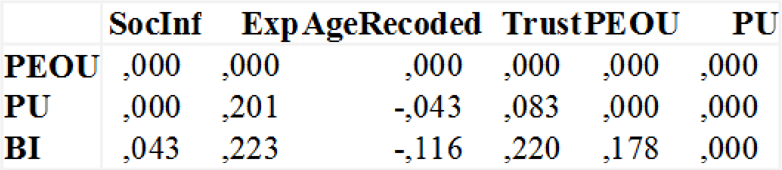
After removing Attitude, the results show that the effect of Age on PEOU (H5b), the effect of Experience on PU (H6a), and the effect of Social Influence on PU (H7a) reaches statistical significance at p < 0.01 (Table 13). The remaining hypotheses have p-values lower than 0.001. Therefore, all relationships in this model are accepted.



			Estimate
PEOU	<---	Trust	,216
PEOU	<---	AgeRecoded	-,111
PEOU	<---	Exp	,519
PU	<---	Trust	,324
PU	<---	AgeRecoded	-,175
PU	<---	Exp	,117
PU	<---	SocInf	,094
PU	<---	PEOU	,387
BI	<---	PU	,460
BI	<---	Trust	,419
BI	<---	PEOU	,148

Table 14 Standardized regression weights

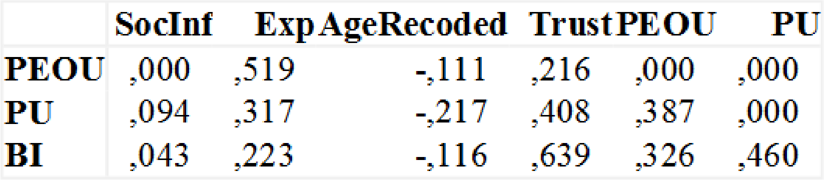
Looking at the standardized β values (Table 14), it is seen that the largest values are Experience on PEOU, PU on BI, Trust on BI, and PEOU on PU.



	SocInf	Exp	AgeRecoded	Trust	PEOU	PU
PEOU	,000	,000	,000	,000	,000	,000
PU	,000	,201	-,043	,083	,000	,000
BI	,043	,223	-,116	,220	,178	,000

Table 15 Standardized indirect effects

From the standardized indirect effects (Table 15), it is found that Experience and Trust have the largest indirect effects on BI. Experience also has a substantial indirect effect on PU through PEOU.



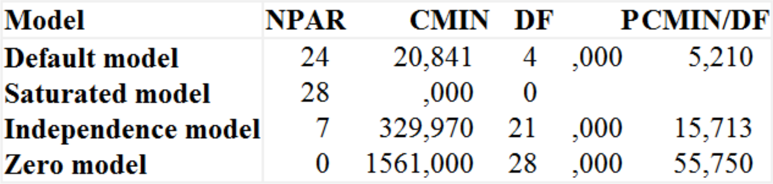
	SocInf	Exp	AgeRecoded	Trust	PEOU	PU
PEOU	,000	,519	-,111	,216	,000	,000
PU	,094	,317	-,217	,408	,387	,000
BI	,043	,223	-,116	,639	,326	,460

Table 16 Standardized total effects

Trust has the largest total effect on BI, with a total effect of 0.639, followed by PU with a total effect of 0.460 (Table 16). Social influence has the lowest total effect on Behavioral Intention (0.043).

Model fit

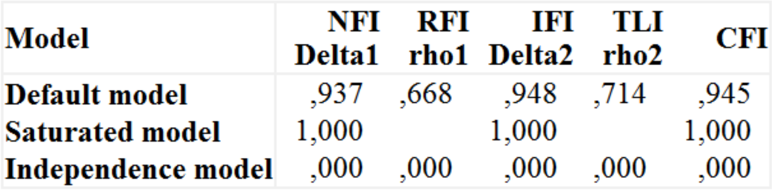
For this new model, the χ^2 value is 20.841, with 4 degrees of freedom. Compared to the validated BioTAM model (66.310, df 9), the χ^2 value is lower, which suggests an increase in model fit. However, the results still show that there is a significant difference between observed and estimated covariance matrices (Table 17).



Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	24	20,841	4	,000	5,210
Saturated model	28	,000	0		
Independence model	7	329,970	21	,000	15,713
Zero model	0	1561,000	28	,000	55,750

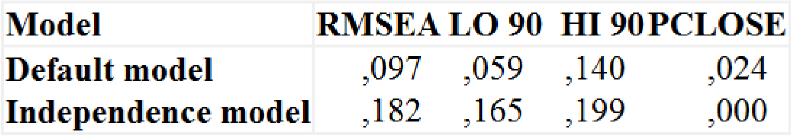
Table 17 Chi-square

The CFI value is 0.945 for this model, which suggests a good model fit (Table 18). The RMSEA value of 0.097 (Table 19) shows a substantial improvement from the model fit of the original BioTAM model (0.479) but should preferably be even lower (below 0.08).



Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,937	,668	,948	,714	,945
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

Table 18 CFI



Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,097	,059	,140	,024
Independence model	,182	,165	,199	,000

Table 19 RMSEA

The extension of BioTAM has improved the model fit, but changes must be made further to improve the χ^2 statistics and RMSEA to acceptable levels. This is discussed in the following section.

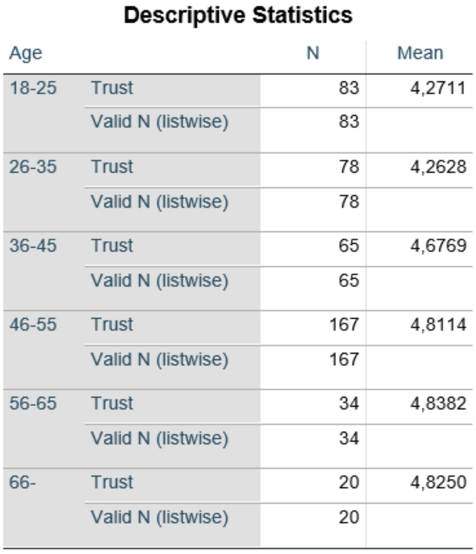
7.4.5 Model 4: Improving model fit

The first measure to improve model fit is to examine the effects of the external factors directly on BI. By doing so, it is found that Experience has a significant direct effect on BI, in addition to an indirect effect through PU and PEOU. There are no significant effects of Age, Gender, and SI on BI.

Next, the effect of external factors on Trust are examined:

Age and Trust

Table 20 shows that there is an increase in the mean value of trust from the age group 18-25 and 26-35 to 36-45. Age group 56-66 has the highest mean value of trust, slightly higher than for the age group 66+.



Descriptive Statistics

Age		N	Mean
18-25	Trust	83	4,2711
	Valid N (listwise)	83	
26-35	Trust	78	4,2628
	Valid N (listwise)	78	
36-45	Trust	65	4,6769
	Valid N (listwise)	65	
46-55	Trust	167	4,8114
	Valid N (listwise)	167	
56-65	Trust	34	4,8382
	Valid N (listwise)	34	
66-	Trust	20	4,8250
	Valid N (listwise)	20	

Table 20 Trust in different age groups

The effect of Age on Trust is statistically significant ($p < 0.001$) and has a standardized β of 0.220 (table 24 and 25).

Experience and Trust

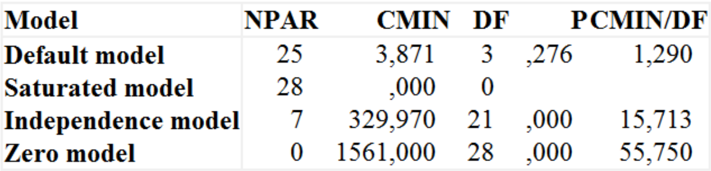
By adding a link between Experience and Trust, it is found that the effect is significant ($p < 0.001$) with a standardized β value of 0.195 (table 24 and 25).

Social Influence and Trust

The results in this thesis show that Social Influence has a significant effect on Trust ($p < 0.001$) with a standardized β value of 0.268 (table 24 and 25).

Model fit

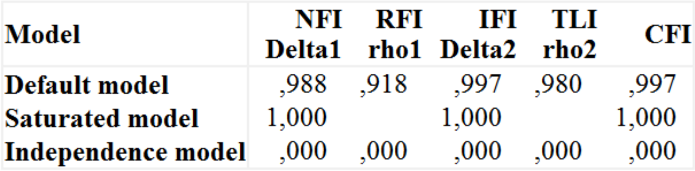
After linking external factors to Trust, the χ^2 value is 3.871, with 3 degrees of freedom (Table 21). The p-value is 0.276, which means that the difference between observed and estimated covariance matrices is insignificant, and there is a good model fit.



Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	25	3,871	3	,276	1,290
Saturated model	28	,000	0		
Independence model	7	329,970	21	,000	15,713
Zero model	0	1561,000	28	,000	55,750

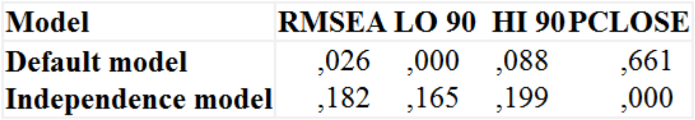
Table 21 New model: Chi-square

The CFI value is 0.997, and RMSEA is 0.026 (Tables 22 and 23). All estimates of model fit indicate that the specified model fits the data observed through the questionnaire. The model fit is highly improved compared to the validated BioTAM model and model 1 in this thesis.



Model	NFI Delta1	RFI rho1	IFI Delta2	TLI rho2	CFI
Default model	,988	,918	,997	,980	,997
Saturated model	1,000		1,000		1,000
Independence model	,000	,000	,000	,000	,000

Table 22 New model: CFI



Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	,026	,000	,088	,661
Independence model	,182	,165	,199	,000

Table 23 New model: RMSEA

7.4.6 Comparison of model fit

The model below compares the model fit between the validated BioTAM model (from this thesis) and the final model (model 4). The model fit is highly increased by extending the model. Model 4 is illustrated on the next page.

	Validated BioTAM	**Model 4**
R Squared for BI	0.69	0.70
Chi Square/ p-value	103.323, 1 df / >0.01	3.871, 3df /0.276
CFI	0.537	0.997
RMSEA	0.479	0.026

7.4.6 Model 4 - Factors that affect acceptance of BASs

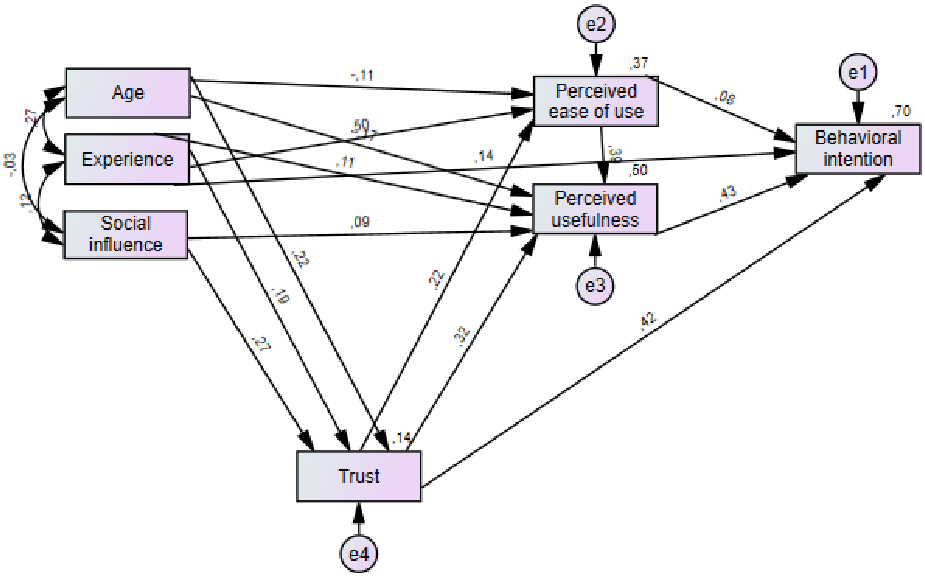
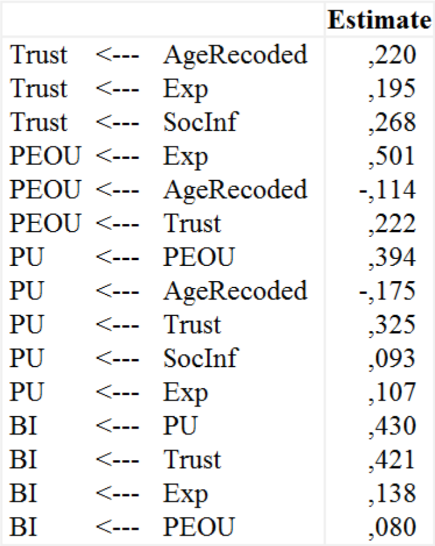


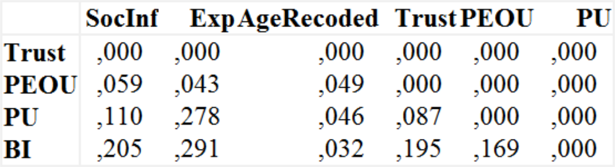
Figure 13 Testing the effect of external factors on trust (model 4)

The factors with the highest direct effect are Experience on PEOU (0.501), PU on BI (0.430), Trust on BI (0.421), and PEOU on PU (0.394) (Figure 13/Table 24). Experience and SI have the most substantial indirect effects on BI, of 0.291 and 0.205, respectively (Table 25).



			Estimate
Trust	<---	AgeRecoded	,220
Trust	<---	Exp	,195
Trust	<---	SocInf	,268
PEOU	<---	Exp	,501
PEOU	<---	AgeRecoded	-,114
PEOU	<---	Trust	,222
PU	<---	PEOU	,394
PU	<---	AgeRecoded	-,175
PU	<---	Trust	,325
PU	<---	SocInf	,093
PU	<---	Exp	,107
BI	<---	PU	,430
BI	<---	Trust	,421
BI	<---	Exp	,138
BI	<---	PEOU	,080

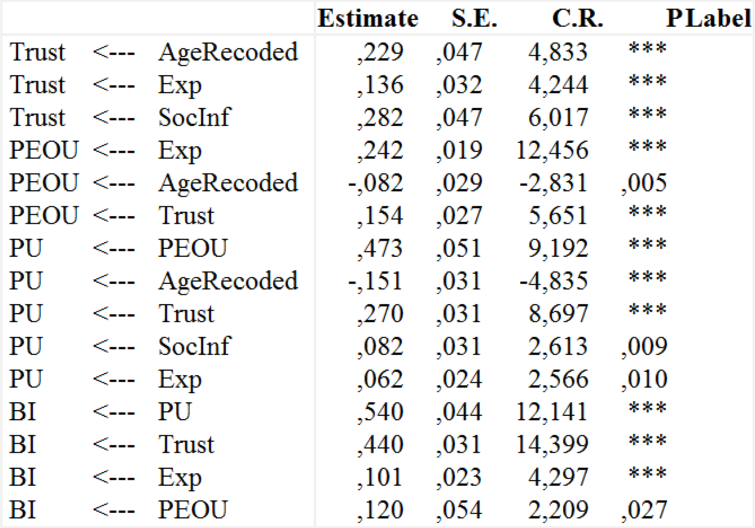
Table 24 Standardized regression weights



	SocInf	Exp	AgeRecoded	Trust	PEOU	PU
Trust	,000	,000	,000	,000	,000	,000
PEOU	,059	,043	,049	,000	,000	,000
PU	,110	,278	,046	,087	,000	,000
BI	,205	,291	,032	,195	,169	,000

Table 25 Standardized indirect effects

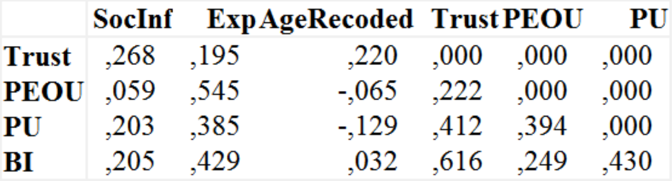
The effect of PEOU on BI and the effect of Experience on PU are significant at p < 0.05. The effect of SI on PU and the effect of Age on PEOU are significant at p < 0.01. The remaining hypotheses have p-values < 0.001 (table 26).



			Estimate	S.E.	C.R.	P	Label
Trust	<---	AgeRecoded	,229	,047	4,833	***	
Trust	<---	Exp	,136	,032	4,244	***	
Trust	<---	SocInf	,282	,047	6,017	***	
PEOU	<---	Exp	,242	,019	12,456	***	
PEOU	<---	AgeRecoded	-,082	,029	-2,831	,005	
PEOU	<---	Trust	,154	,027	5,651	***	
PU	<---	PEOU	,473	,051	9,192	***	
PU	<---	AgeRecoded	-,151	,031	-4,835	***	
PU	<---	Trust	,270	,031	8,697	***	
PU	<---	SocInf	,082	,031	2,613	,009	
PU	<---	Exp	,062	,024	2,566	,010	
BI	<---	PU	,540	,044	12,141	***	
BI	<---	Trust	,440	,031	14,399	***	
BI	<---	Exp	,101	,023	4,297	***	
BI	<---	PEOU	,120	,054	2,209	,027	

Table 26 p-values

Trust is by far the largest contributor to explaining the variance in BI, with a standardized total effect of 0.616, followed by PU (0.430) and Experience (0.429). Age has the lowest total effect, with a B value of 0.032 (table 27).



	SocInf	Exp	AgeRecoded	Trust	PEOU	PU
Trust	,268	,195	,220	,000	,000	,000
PEOU	,059	,545	-,065	,222	,000	,000
PU	,203	,385	-,129	,412	,394	,000
BI	,205	,429	,032	,616	,249	,430

Table 27 Standardized total effects

7.5 Trust in different actors in the market

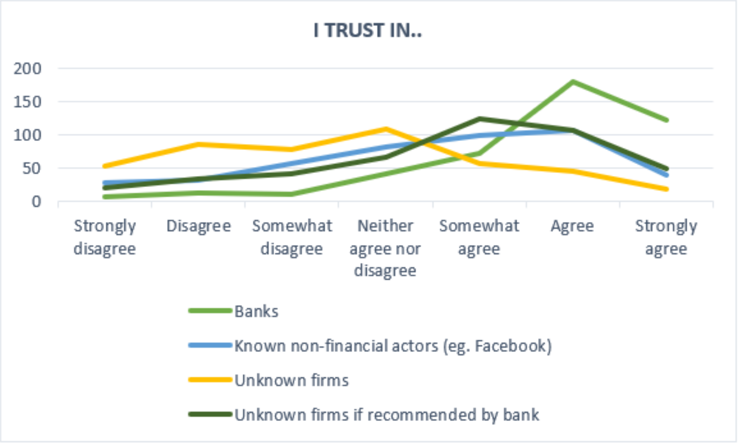


Figure 14 Trust in different actors

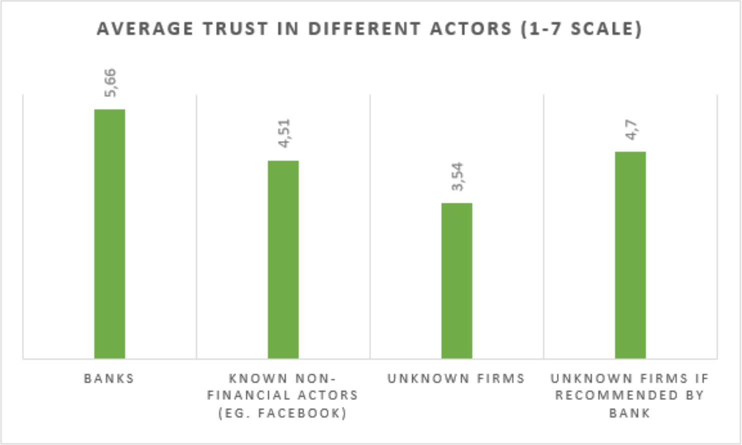


Figure 15 Average trust in actors

The results show that there is a large difference in the trust of different actors in the financial sector. Figure 14 compares the distribution of responses about trust in the different actors asked about in the questionnaire, while figure 15 shows the average scores for each. The results show that the incumbent banks are seen as the most trustworthy in the market. The consumers trust the unknown fintech startups the least, but the trust is highly increased if their bank recommends the firm. There is some disagreement about the trust in BigTechs, but the average score is in the middle of the scale (below banks and unknown firms recommended by banks).

7.6 Summary of hypotheses testing

H1: A positive attitude towards biometric technology has a positive effect on behavioral intention	NS
H2: Perceived usefulness has a positive effect on attitude	S_1**
H3: Perceived ease of use has a positive effect on attitude	NS
H4a: Gender has a significant effect on perceived usefulness / b: Gender has a significant effect on perceived ease of use	NS / NS
H5a: Increasing age will have a negative effect on perceived usefulness / b: Increasing age will have a negative effect on perceived ease of use	S** / S*
H6a: Experience has a positive effect on perceived usefulness / b: Experience has a positive effect on perceived ease of use	S** / S**
H7a: Social influence affects perceived usefulness / b: Social influence affects perceived ease of use	S* / NS
H8a: Trust has a positive effect on attitude / b: Trust has a positive effect on behavioral intention	S** / S**

Note: NS = not supported, S = supported, * = significant at 0.01 level, ** = significant at 0.001 level, $_1$ =significant, but removed because H1 was rejected.

Also, it is found that positive social influence, experience, and increasing age has a positive impact on trust. Experience also has a significant direct effect on behavioral intention. All these additional links are significant at 0.001 level.

8 Discussion

In the current thesis, the goal is to confirm the findings of Kanak and Sogukpinar (2017), and to strengthen the model by adding attitude and the external factors “gender”, “age”, “experience”, and “social influence”.

The findings are quite interesting, and a higher number of respondents strengthens the BioTAM model by Kanak and Sogukpinar (2017). After removing the insignificant relationships and constructs from the proposed model, the model fit is improved by exploring the effect of external factors further, ending up with model 4. The findings are discussed in light of relevant literature below.

8.1 The role of attitude on acceptance of biometric technologies

Before data collection, it was believed that the inclusion of an attitude construct could strengthen the acceptance model. What is interesting in the results (model 2) is that Trust and PU has a significant effect on attitude towards biometric technology; however, people’s attitude does not influence their behavioral intention to use these biometric technologies.

Because attitude is not found to have a significant effect on behavioral intention (model 2), it is removed from the model. This result is consistent with the findings from Cheng, Lam and Yeung (2006), where they find that attitude shows an insignificant effect on behavioral intention, but contradicts the findings of Boonsiritomachai and Pitchayadejanant (2017).

The results can be influenced by choice of analysis, as López-Bonilla and López-Bonilla (2017) find that TAM-R is better when CB-SEM is used. Further research should verify the results using VB-SEM.

Even though attitude is perceived by many as an essential factor to describe human behavior, several researchers have disregarded the attitude construct in the context of IT adoption. As a result, this construct is often omitted in the field of IT adoption (Cheng, Lam and Yeung, 2006; Kim, Chun and Song, 2009). The findings in this thesis support this.

A Senior Business Developer from DNB, interviewed by Got, Andresen and Granberg (2016, p. 62, Translated from Norwegian), said that “nobody thinks that it’s fun to pay; so the solutions must be simple, fast, and at the same time secure”. This is consistent with the findings in this thesis, where the results show that it does not matter if the technology is fun or exciting to use, or if it gives the user a positive experience. What matters is that the technology is easy to use, useful, and safe with regards to privacy and security.

This finding implies that FinTech developers should not use too much time trying to make banking and payment solutions fun and entertaining, but instead focus on making simple solutions and ensure privacy and security.

8.2 The role of sex on acceptance of biometric technologies

Based on significant results in previous research (Chawla and Joshi, 2018; Zhang, Nyheim and S. Mattila, 2014), the role of sex on the acceptance of biometric technology is tested in this thesis. The results show that there is no significant difference between how men and women perceive ease of use and usefulness of biometric technologies (model 1). This result confirms the findings of Padilla-Meléndez, del Aguila-Obra and Garrido-Moreno (2013) and Hernández, Jiménez and Martin (2011, as cited in Chawla and Joshi (2018)).

It is suggested by Chawla and Joshi (2018) that the differences between genders are more significant in countries with higher gender differences and stereotypical gender roles. However, the differences between genders are believed to significantly reduce in the time to come, as the differences are diminishing and equality increasing. Norway ranked second on the Global Gender Gap Index 2020 rankings (World Economic Forum, 2019), which might suggest why the results show no significant differences between genders.

8.3 The role of age on acceptance of biometric technologies

Before the study, it was believed that an increase in age would have an exclusively negative impact on acceptance towards biometric technologies. Surprisingly, results show that the total effect of age on behavioral intention is very low (model 4). The total effect is low because increasing age has a positive effect on some factors and a negative effect on other factors affecting behavioral intention. Trust is higher among older individuals than younger, so increasing age has a positive direct effect ($\beta = 0.220$) on trust. On the other hand, younger people perceive BASs as more useful than older people, which means that increasing age has a negative effect on perceived usefulness ($\beta = -0.175$). Increasing age also has a negative effect on perceived ease of use ($\beta = -0.114$), because younger persons find the technology easier to use than the older.

In other words, even if older people find the technology harder to use and see fewer benefits of using it, they trust the technology more than younger people. As discussed earlier, Niehaves and Plattfaut (2017) find that older people are more hesitant to adopt technology. This contradicts the findings of this thesis, where the positive effect of age on trust reduces the negative effect of age on PU and PEOU.

Interestingly, the findings by Fungáčová, Hasan and Weill (2019) are the complete opposite of the findings in this study. Fungáčová, Hasan and Weill (2019) find that trust decreases as age increases.

According to Utdanningsforbundet (2017), it is found that the level of trust is increasing as the age increases until the age group 45-66, where it exhibits a plateau (or even decreases slightly). This is also true for the level of trust in this thesis. The reason might be that younger people are more updated on privacy and security risks, and therefore have less trust in the technology.

The negative effect of increasing age on PU and PEOU can be caused by technology-anxiety, as discussed by Chawla and Joshi (2018). As today's technology is getting more and more advanced, people struggle to tag along. According to Utheim (2013), a survey by Carat find that more than one in four find technology too complicated, and the elderly are among the tech-losers. It is also normal to lose some of the cognitive abilities as one grows older. This can impact elderlies in their decision-making and increase trust as they lack knowledge about fraud and technology (Stranden, 2017).

According to the results of this thesis, providers of new technological solutions should offer seminars or other ways of training the elderly to increase PEOU and PU (if the elderly are part of the target group). When targeting younger consumers, transparency with regards to privacy and security is essential, as this might increase the chance of adoption.

8.4 The role of experience on acceptance of biometric technologies

Before data collection and analysis, the assumption was that experience would have a positive impact on PU and PEOU, as is found by Alambaigi and Ahangari (2015) and Irani (2000). The findings in this thesis confirm this, and also, it is found that experience directly influences trust and BI.

Experience with biometric technologies has an important role in a person's acceptance of similar technologies. The results in the final model (model 4) show that experience is among the factors that, in total, influence behavioral intention most, only exceeded by perceived usefulness and trust. What is particularly interesting is the significant effect experience has on trust.

An anonymous professor, interviewed by Rainie and Anderson (2017, p. 61), explains that "trust is built exclusively on perception" and that "increased experience with a thing gives them greater trust, even when it is not deserved". Bart Knijnenburg, assistant professor in human-centered computing at Clemson University, is also asked about experience and trust by Rainie and Anderson (2017). He responds that even though the privacy and security threats are likely to increase in the coming years, the trust will still increase because people will be more and more required to use new technologies, and thus they become more familiar with the technology. Also, Chawla and Joshi (2018) suggest that there is an effect of experience on trust because trust takes time to build.

Limited research on the direct effect of experience on BI is found. However, a plausible reason for this significant effect can be that experience with a technology reduces the "entry barrier" of adopting similar technologies. Research conducted by Szajna (1996) also shows that prior experience strengthens the relationship between intention to use and actual use.

Based on this result, developers should consider experience and familiarity when designing new biometric payment solutions. According to a report conducted by Elkjøp (2019) about "digital outsiders", one out of three Norwegians struggle to keep up with the technological development. Solbak (2019), from Eplehjelp, explains how many people feel that new technology creates a lot of frustration and despair, even though the purpose of the technology is to make the consumers' lives easier. Thus, if the goal of a technology developer is to appeal to a mass market, it can be risky to deviate too far from previous solutions.

8.5 The role of social influence on acceptance of biometric technologies

As discussed earlier in this thesis, the effect of social influence on technology acceptance is highly debated, and researchers examining this construct find both significant and insignificant relationship. It was expected that social influence affects PU and PEOU; however, the results show that the effect of social influence on perceived ease of use is not significant, and there is only a small, but significant effect of social influence on perceived usefulness.

Merhi, Hone and Tarhini (2019), when comparing consumers in England and Lebanon, discusses how there is a difference in the effect of social influence based on how high or low the country scores on Hofstede’s dimension of individualism. They find that Lebanon, which scores low on individualism, regard the opinions of their social network higher than England, which scores high on individualism. Norway is considered an Individualist society, which might explain why the effect of social influence on PU and PEOU is insignificant or low (Hofstede Insights, n.d.).

What is new in this study, however, is that a strong and significant effect of social influence on trust is found. Similar findings can be found in other fields:

Beyari and Abareshi (2018) discussed the relationship between social influence and trust in the context of social commerce and found that there exists a strong relationship between them. The reason for this, according to the researchers, is that a consumer will trust a specific technology more if (s)he receives information and recommendations from friends and family.

Wei, Zhao and Zheng (2019) use psychological and neuroscientific methods to examine the effect of social influence on the level of trust in the context of a trust game. They find that people tend to listen to the opinions of peers and that the level of trust is significantly higher compared to the baseline condition when the majority of group members trust the trustee. The concept of “social conformity” is a phenomenon where people adopt the opinions, judgments, and behavior of others, even if these are against the person's preference (Wei, Zhao and Zheng, 2019).

Of the external factors included in this thesis, social influence is the factor with the highest effect on trust. The results show that family and friends can affect a person’s trust in technology and their perception of benefits of using the technology, however, family and friends do not influence a person’s perception of how easy the technology is to use.

As a result, FinTech companies and other financial and non-financial institutions do not necessarily need to gain the trust of all potential users to get consumers to adopt their solutions, but can use ambassadors that people trust and rely on word-of-mouth.

8.6 The importance of institutional trust

Trust is found to be the highest influencer of a consumer’s choice of adopting a biometric technology, both in this thesis and other research including trust (Miltgen, Popovič and Oliveira, 2013; Sharma, 2017). Developing novel technologies alone is not enough to succeed and to get people to use the product – the trust in both the company and the technology is equally important (PwC, n.d.).

According to PwC (n.d.), trust is a crucial factor when developing new technology, and the higher the trust in a given company, the higher the chance of consumers adopting that company’s products when it is introduced. The actors with the highest trust in the market are those who ensure privacy and who make ethical considerations (PwC, n.d.). This might be the reason why incumbent banks score the highest on trust in the survey conducted for this thesis; Norwegian banks are subject to strict guidelines and regulations from the Financial Supervisory Authority (Regjeringen, n.d.), in addition to European regulations such as GDPR and PSD2. The incumbent banks have often also operated for years and are well-known by the consumers because they have used these banks their whole lives. This is also consistent with the theory of Merhi, Hone and Tarhini (2019), that institutional trust is created from prior experience with the company and its reputation.

PwC (n.d.) has some suggestions on how to increase the trust of a company: first, the company must ensure the user’s privacy and provide the user with information about how their data is treated and used. The user must be given access to information so that it is visible that the company is acting according to laws and regulations. Second, alliances can be beneficial for new fintech startups. The results in this thesis show that the trust of unknown companies is highly increased (from a mean score of 3.54 to 4.70) if credible incumbent banks recommend them.

9 Conclusion

9.1 Main findings

An extension of the model BioTAM, developed for new generation BASs, is proposed in this study to explain consumer's acceptance of biometric solutions used in FinTech. This subject is highly relevant following the implementation of PSD2, as the financial market is likely to see many new actors in the time to come. Because the implementation of this regulation is still relatively new, there is limited research on how different financial and non-financial market actors can affect technology acceptance of financial technologies.

This thesis confirms the findings of several other technology acceptance research about trust being the highest influencer of a consumer's decision to adopt a technology. Trust is particularly important in the field of biometrics, as biometric traits are considered as highly sensitive data, referred to as "special categories of personal data" in GDPR (Gemalto, 2020a).

This thesis consists of two research questions:

(1) Can BioTAM be validated with a larger sample?

The BioTAM model, proposed by Kanak and Sogukpinar (2017) as a proof-of-concept, is subject to validation with an increased number of respondents and an improved scale. All hypotheses from BioTAM are accepted ($p < 0.001$), and the model explains 69 percent of the variance in behavioral intention, which is a substantial increase from the original study. However, BioTAM has a poor model fit.

(2) Do external factors influence the acceptance of biometric technologies in the financial sector?

The BioTAM model is extended with the external factors "sex", "age", "experience", and "social influence", which are factors that can also be found in other technology acceptance models, such as UTAUT. In this thesis, it is found that "age", "experience", and "social influence" have significant effects on technology acceptance.

What is new in these results is that the assumption that increasing age exclusively has a negative effect on technology acceptance is wrong. Increasing age has a negative effect on the perceived usefulness and perceived ease of use, but a positive effect on trust. Because of this, it is found that the total effect of age is minimal. Providers of biometric FinTech can use this information to target different age groups correctly: focus on usefulness and training among older users and focus on privacy and security among younger users.

Social influence is a debated factor in technology acceptance studies. However, for biometrics in FinTech among Norwegian consumers, it is found that social influence has a positive effect on both trust and perceived usefulness. This information can be beneficial for providers of technological solutions because they can, for example, use ambassadors and influencers in their marketing.

Experience is the only external factor that positively influences all dependent variables (perceived usefulness, perceived ease of use, behavioral intention, and trust) in the model (model 4). It thus has a strong total effect on behavioral intention to use biometric technologies.

In addition to these two research questions, this thesis offers new information about trust in different types of actors in the market. The level of trust in three different actors is compared: traditional banks, BigTechs, and FinTech startups.

The results show that traditional banks are perceived as most trustworthy, not surprising, considering consumers' familiarity with these, and their good reputation. Traditional banks are followed by BigTechs, with a difference of 1.15 in average trust score (scale 1-7). The least trusted actors are the FinTech startups, who the consumers have no experience with. The trust in startups has an average score of 2.12 lower than traditional banks and 0.97 lower than BigTechs. However, if startups enter an alliance with a traditional bank, the level of trust increases, and it passes the BigTechs (0.19 higher average trust score than BigTechs). Thus, FinTech startups can overcome their weakness of being unknown and not trusted by consumers by entering an alliance with an institution that is known and trusted.

9.2 Limitations and further research

The proposed model defines behavioral intention as the outcome variable and does not cover the actual use of BASs due to practical limitations. Adding actual use could be highly interesting for further research when possible.

The data was mainly collected in Møre og Romsdal. It would be interesting to obtain more respondents from the less represented counties, especially Northern Norway, as a report done by DNX Studio (n.d.) states that there are differences in municipalities (especially north vs. south) regarding the residents' opinion towards technology and trust.

Since both researchers work in a bank, large parts of our networks are also bank employees. This can affect the responses.

The biometric technologies mentioned in the questionnaire is limited to the financial sector only, and an investigation of this model in other industries would be interesting for further research.

The questionnaire was published in the early stage of Covid-19. Of consideration to infection prevention, there has been a large focus on contactless payments and Apple/Google Pay (and similar solutions) in the media. Because of this, the responses in the questionnaire might be different if the same questions are republished today. It could be an interesting subject for further research to examine how Covid-19 has impacted people’s opinions towards biometric technologies in FinTech.

Regarding social influence, the questions are asked directly. For further research, it would be interesting to reformulate these questions to measure unconscious social influence, to avoid bias from the respondents.

Most data in previous empirical research do not meet the assumptions of normality, as applies to the data in this study. A decision was made not to remove any variables based on the non-normal distribution, and this might have caused limitations to the study. Non-normality can cause a disturbance in the analysis, which might impact the results achieved.

The use of AMOS and CB-SEM can affect the results with regards to attitude (López-Bonilla and López-Bonilla, 2017), and further research should validate these findings using, for example, SmartPLS.

References

Al-falluji, R. A. A. (2015) A Survey of Biometrics: Features, Components, Examples and Applications, *International Journal of Advanced Research in Computer and Communication Engineering*, 4(9), pp. 221-226. doi: 10.17148/IJARCCE.2015.4948.

Alalwan, A. A. *et al.* (2018) Examining adoption of mobile internet in Saudi Arabia: Extending TAM with perceived enjoyment, innovativeness and trust, *Technology in Society*, 55, pp. 100-110. doi: 10.1016/j.techsoc.2018.06.007.

Alambaigi, A. and Ahangari, I. (2015) Technology Acceptance Model (TAM) As a Predictor Model for Explaining Agricultural Experts Behavior in Acceptance of ICT, *International Journal of Agricultural Management and Development*, 6(2), pp. 235-247.

Asadi, S. *et al.* (2017) Customers perspectives on adoption of cloud computing in banking sector, *Information Technology and Management*, 18(4), pp. 305-330. doi: 10.1007/s10799-016-0270-8.

Aware Inc (2019) *Biometrics on the Road to Automotive Identity*. Available at: https://www.aware.com/blog-biometrics-on-the-road-to-automotive-identity/ (Accessed: 16 April 2020).

BankID (n.d.) *Historien. Så langt.* Available at: https://www.bankid.no/privat/om-oss/ (Accessed: 28 June 2020).

Beal, V. (n.d.) *False Acceptance*. Available at: https://www.webopedia.com/TERM/F/false_acceptance.html (Accessed: 22 March 2020).

Belguechi, R., Cherrier, E. and Rosenberger, C. (2012) *Texture based fingerprint BioHashing: Attacks and robustness*. Unpublished paper presented at 2012 5th IAPR International Conference on Biometrics (ICB).

Beyari, H. and Abareshi, A. (2018) The Interaction of Trust and Social Influence Factors in the Social Commerce Environment, *International Conference of Reliable Information and Communication*. ResearchGate: Springer Nature Switzerland AG.

Bhalla, D. (n.d.) *Standardized vs unstandardized regression coefficient*. Available at: https://www.listendata.com/2015/04/standardized-vs-unstandardized.html (Accessed: 30 June 2020).

Biometric Institute (n.d.) *Biometrics definition*. Available at: https://www.biometricsinstitute.org/what-is-biometrics/ (Accessed: 21 February 2020).

Biometric technology today (2018) Mastercard and Visa make major push with biometric cards, *Biometric Technology Today*, 2018(2), pp. 1-2. doi: 10.1016/s0969-4765(18)30015-8.

Biometric Technology Today (2019) University develops ID system using ear canal, *Biometric Technology Today*, 2019(9), pp. 11-12. doi: 10.1016/S0969-4765(19)30130-4.

Biometric Technology Today (2020) Kaspersky reports surge in cyber-attacks on selfies and other biometry, *Biometric Technology Today*, 2020(1), pp. 1-2. doi: 10.1016/s0969-4765(20)30001-1.

Boonsiritomachai, W. and Pitchayadejanant, K. (2017) Determinants affecting mobile banking adoption by generation Y based on the Unified Theory of Acceptance and Use of Technology Model modified by the Technology Acceptance Model concept, *Kasetsart Journal of Social Sciences*. doi: 10.1016/j.kjss.2017.10.005.

Boughzala, I. (2014) How Generation Y Perceives Social Networking Applications in Corporate Environments *Integrating Social Media into Business Practice, Applications, Management, and Models.* Researchgate, pp. 163-181.

Browne, R. (2020) Big Tech will push deeper into finance this year — but avoid the 'headache' of being a bank, *CNBC*. Available at: https://www.cnbc.com/2020/01/03/big-tech-will-push-into-finance-in-2020-while-avoiding-bank-regulation.html.

Burt, C. (2019) *Trulioo powers biometric digital identity verification offering from Refinitiv*. Available at: https://www.biometricupdate.com/201909/trulioo-powers-biometric-digital-identity-verification-offering-from-refinitiv (Accessed: 15 May 2020).

Bülbül, D. (2013) Determinants of trust in banking networks, *Journal of Economic Behavior & Organization*, 85, pp. 236-248. doi: 10.1016/j.jebo.2012.02.022.

Chawla, D. and Joshi, H. (2018) The Moderating Effect of Demographic Variables on Mobile Banking Adoption: An Empirical Investigation, *Global Business Review*, 19(3_suppl), pp. S90-S113. doi: 10.1177/0972150918757883.

Cheng, T. C. E., Lam, D. Y. C. and Yeung, A. C. L. (2006) Adoption of internet banking: An empirical study in Hong Kong, *Decision Support Systems*, 42(3), pp. 1558-1572. doi: https://doi.org/10.1016/j.dss.2006.01.002.

China Daily (2019) China's first facial recognition payment-based shopping street opens in Wenzhou, *China Daily*. Available at: http://www.chinadaily.com.cn/a/201901/18/WS5c4142c7a3106c65c34e53dd.html.

Computer Hope (2019) *Voice recognition*. Available at: https://www.computerhope.com/jargon/v/voicreco.htm (Accessed: 25 March 2020).

Datatilsynet (2019) *Biometri*. Available at: https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/biometri/ (Accessed: 5 June 2020).

Davcik, N. S. (2014) The use and misuse of structural equation modeling in management research, *Journal of Advances in Management Research*, 11(1), pp. 47-81. doi: 10.1108/jamr-07-2013-0043.

Davies, S. *et al.* (2016) *Global FinTech Survey 2016*. PwC. Available at: https://www.pwc.com/gx/en/financial-services/fintech/assets/fin-tech-banking-2016.pdf (Accessed: 28 June 2020).

Davis, F. (1989) Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *Management Information Systems Quarterly*, 13(3), pp. 319-340.

DNB (n.d) *New regulatory framework for payment services*. Available at: https://www.dnb.no/en/business/transaction-banking/cash-management/articles/psd2.html (Accessed: 24 June 2020).

DNX Studio (n.d.) *Ny undersøkelse: Slik er nordmenns tilit til makt og teknologi*. Available at: https://www.dn.no/annonsorinnhold/ny-undersokelse-slik-er-nordmenns-tillit-til-makt-og-teknologi/2-1-394268 (Accessed: 18 June 2020).

Elkjøp (2019) *Én av tre nordmenn henger ikke med*. Available at: http://pressroom.elkjop.no/pressreleases/en-av-tre-nordmenn-henger-ikke-med-2905220.

Elliott, S. J., Massie, S. A. and Sutton, M. J. (2007) The Perception of Biometric Technology: A Survey (pp. 259-264). doi: 10.1109/AUTOID.2007.380630.

European Commission (2019) *The Digital Economy and Society Index (DESI)*.

Finans Norge and Kantar TNS (2018) *Forbruker- og finanstrender 2018*. Available at: https://www.finansnorge.no/aktuelt/nyheter/forbruker-og-finanstrender/forbruker--og-finanstrender-2018/forbruker--og-finanstrender-2018/.

Finans Norge (2019) *PSD2 eller betalingstjenestedirektivet*. Available at: https://www.finansnorge.no/tema/bank/psd2-eller-betalingstjenestedirektivet/ (Accessed: 21 April 2020).

Finaut (n.d) *PSD2 er rett rundt hjørnet, men hva betyr det egentlig*. Available at: https://www.finaut.no/artikler/2019/psd2-er-rett-rundt-hjornet-men-betyr-det-egentlig/ (Accessed: 21 April 2020).

Findbiometrics (2019) *Biometric Authentication is Key to Success in a Post PSD2 Landscape: Report*. Available at: https://findbiometrics.com/biometric-authentication-psd2-503205/ (Accessed: 21 April 2020).

Findbiometrics (n.d.) *Iris Recognition*. Available at: https://findbiometrics.com/solutions/iris-scanners-recognition/ (Accessed: 4 March 2020).

Fjørtoft, L. E. (n.d.) *PSD2 er starten på en ny fremtid for bankene*. Available at: https://www.pwc.no/no/bransjer/bank-og-finans/psd2.html (Accessed: 24. February 2020).

Frost, J. (n.d.) *How High Does R-squared Need to Be?* Available at: https://statisticsbyjim.com/regression/how-high-r-squared/ (Accessed: 31 March 2020).

Fungáčová, Z., Hasan, I. and Weill, L. (2019) Trust in banks, *Journal of Economic Behavior & Organization*, 157, pp. 452-476. doi: https://doi.org/10.1016/j.jebo.2017.08.014.

Gatali, I. F. *et al.* (2016) *A qualitative study on adoption of biometrics technologies*. Unpublished paper presented at Proceedings of the 18th Annual International Conference on Electronic Commerce e-Commerce in Smart connected World - ICEC '16.

Gemalto (2020a) *Biometric data and data protection regulations (GDPR and CCPA)*. Available at: https://www.gemalto.com/govt/biometrics/biometric-data (Accessed: 21 April 2020).

Gemalto (2020b) *Biometrics: authentication & identification*. Available at: https://www.gemalto.com/govt/inspired/biometrics (Accessed: 21 February 2020).

Ghaderi, H. (2019) *Vipps nær 100 millioner i underskudd*. Available at: https://e24.no/naeringsliv/i/wPVaeM/vipps-naer-100-millioner-i-underskudd (Accessed: 30 June 2020).

Giske, M. E. (2019) *Blunk! så har du betalt*. Available at: https://www.dnb.no/dnbnyheter/no/din-okonomi/blunk-sa-har-du-betalt (Accessed: 8 June 2020).

Global Security (2011) *Emerging Biometric Technologies*. Available at: https://www.globalsecurity.org/security/systems/biometrics-emerging.htm (Accessed: 18 December 2019 2019).

Got, C. W., Andresen, J. B. and Granberg, K. E. (2016) *Fremtidens betaling - en scenarioanalyse*, Handelshøyskolen ved HiOA. Available at: https://fagarkivet.oslomet.no/nb/item/asset/dspace:4508/kand340_kand320_kand_412_%C3%98ABAC3900_200516.pdf (Accessed: 20 June 2020).

Guillaume, B. and Horesnyi, E. (2019) *PSD2 Open up or disappear?* Available at: https://www.soprabanking.com/insights/psd2-open-up-or-disappear/ (Accessed: 5 June 2020).

Hair Jr., J. *et al.* (2019) *Multivariate Data Analysis*. 8 edn. Hampshire: Cengage Learning, EMEA.

Hofstede Insights (n.d.) *Country comparison*. Available at: https://www.hofstede-insights.com/country-comparison/norway,the-uk/ (Accessed: 21 April 2020).

HSBC (n.d.) *Voice ID*. Available at: https://ciiom.hsbc.com/ways-to-bank/phone-banking/voice-id/ (Accessed: 30 June 2020 2020).

Idexbiometrics (2020) *How the COVID-19 Pandemix is Bringing Biometric Identification One Step Closer*. Available at: https://www.idexbiometrics.com/how-the-covid-19-pandemic-is-bringing-biometric-identification-one-step-closer/ (Accessed: 8 june 2020).

Idexbiometrics (n.d) *About Idex Biometrics*. Available at: https://www.idexbiometrics.com/about-idex/ (Accessed: 29 May 2020).

ievo (2019) *Biometrics and the GDPR: Why you should adopt the technology*. Available at: https://ievoreader.com/biometrics-and-the-gdpr-why-you-should-adopt-the-technology/ (Accessed: 5 June 2020).

IKT Norge (n.d.) *Norsk Fintech på vei ut i verden*. Available at: https://www.ikt-norge.no/norsk-fintech-pa-vei-ut-i-verden/ (Accessed: 27 June 2020).

Irani, T. (2000) Prior Experience, Perceived Usefulness and the Web: Factors Influencing Agricultural Audiences' Adoption of Internet Communication Tools, *Journal of Applied Communications*, 84(2). doi: 10.4148/1051-0834.2151.

iResearchNet (n.d.) *Hedonic Theory*. Available at: http://psychology.iresearchnet.com/sports-psychology/health-promotion/hedonic-theory/ (Accessed: 18 April 2020).

Islam, M. F. *et al.* (2019) Perception and prediction of intention to use online banking systems, *International Journal of Research in Business and Social Science (2147- 4478)*, 9(1), pp. 112-116. doi: 10.20525/ijrbs.v9i1.591.

Kaasbøll, J. (2009) *Technology Acceptance Model*. Available at: https://www.uio.no/studier/emner/matnat/ifi/nedlagte-emner/TOOL1100/h09/TAM.pdf (Accessed: 2 March 2020).

Kanak, A. and Sogukpinar, I. (2014) BioPSTM: a formal model for privacy, security, and trust in template-protecting biometric authentication, *Security and Communication Networks*, 7(1), pp. 123-138. doi: 10.1002/sec.626.

Kanak, A. and Sogukpinar, I. (2017) BioTAM: a technology acceptance model for biometric authentication systems, *The Institution of Engineering and Technology*, 6(6), pp. 457-467. doi: 10.1049/iet-bmt.2016.0148.

Kawakami, T. (2020) *Coronavirus gives China more reason to employ biometric tech*. Available at: https://asia.nikkei.com/Business/China-tech/Coronavirus-gives-China-more-reason-to-employ-biometric-tech (Accessed: 29 May 2020).

Kim, Y. J., Chun, J. U. and Song, J. (2009) Investigating the role of attitude in technology acceptance from an attitude strength perspective, *International Journal of Information Management*, 29(1), pp. 67-77. doi: 10.1016/j.ijinfomgt.2008.01.011.

Le, D. T. *et al.* (2018) Technology Acceptance and Future of Internet Banking in Vietnam, *Foresight and STI Governance*, 12(2), pp. 36-48. doi: 10.17323/2500-2597.2018.2.36.48.

Lee, D. Y. and Lehto, M. R. (2013) User acceptance of YouTube for procedural learning: An extension of the Technology Acceptance Model, *Computers & Education*, 61, pp. 193-208. doi: https://doi.org/10.1016/j.compedu.2012.10.001.

Lekkas, N. (n.d) *The Big Five Tech Companies: Infographic & History*. Available at: https://growthrocks.com/blog/big-five-tech-companies-acquisitions/ (Accessed: 21 June 2020).

Lim, M. H. and Yuen, P. C. (2016) Entropy Measurement for Biometric Verification Systems, *IEEE Trans Cybern*, 46(5), pp. 1065-1077. doi: 10.1109/TCYB.2015.2423271.

López-Bonilla, L. M. and López-Bonilla, J. M. (2017) Explaining the discrepancy in the mediating role of attitude in the TAM, *British Journal of Educational Technology*, 48(4), pp. 940-949. doi: 10.1111/bjet.12465.

Lorvik, N. (2019) På denne kafeen kan du betale med ansiktet ditt, *Nettavisen*, 27 June 2019. Available at: https://www.nettavisen.no/okonomi/pa-denne-kafeen-kan-du-betale-med-ansiktet-ditt/3423806565.html.

Lovdata (2019) *Personopplysningsloven*. Available at: https://lovdata.no/dokument/NL/lov/2018-06-15-38 (Accessed: 5 June 2020).

Mansour, K. B. (2016) An analysis of business' acceptance of internet banking: an integration of e-trust to the TAM, *Journal of Business & Industrial Marketing*, 31(8), pp. 982-994. doi: 10.1108/jbim-10-2016-271.

MeasuringU (n.d.) *Should you use 5 or 7 point scales?* Available at: https://measuringu.com/scale-points/ (Accessed: 2 July 2020).

Merhi, M., Hone, K. and Tarhini, A. (2019) A cross-cultural study of the intention to use mobile banking between Lebanese and British consumers: Extending UTAUT2 with security, privacy and trust, *Technology in Society*, 59. doi: 10.1016/j.techsoc.2019.101151.

Merriam-Webster (n.d.) *FinTech*. Available at: https://www.merriam-webster.com/dictionary/fintech (Accessed: 21 February 2020).

Miltgen, C. L., Popovič, A. and Oliveira, T. (2013) Determinants of end-user acceptance of biometrics: Integrating the "Big 3" of technology acceptance with privacy context, *Decision Support Systems*, 56, pp. 103-114. doi: 10.1016/j.dss.2013.05.010.

Molstad, K. (2003) Sett finger'n på mobilen, *Aftenposten*, 15 July 2003. Available at: https://www.aftenposten.no/norge/i/dRz2X/sett-fingern-paa-mobilen.

Morosan, C. (2011) Customers' Adoption of Biometric Systems in Restaurants: An Extension of the Technology Acceptance Model, *Journal of Hospitality Marketing & Management*, 20(6), pp. 661-690. doi: 10.1080/19368623.2011.570645.

Mortvedt, F. T. (2017) *Fersk rapport: Norge har enormt potensial innen fintech*. Available at: https://e24.no/teknologi/i/xPlPPV/fersk-rapport-norge-har-enormt-potensial-innen-fintech (Accessed: 12 May 2020).

MyMobileZA (n.d.) *iPhone 5S*. Available at: https://mymobileza.com/product/iphone-5s-refurb-a-grade/ (Accessed: 20 February 2020).

Nestebank (2020) *Banker i Norge*. Available at: https://nestebank.no/banker/ (Accessed: 28 June 2020).

News in Brief (2019), *Biometric Technology Today*, 2019(9), pp. 4. doi: https://doi.org/10.1016/S0969-4765(19)30123-7.

Niehaves, B. and Plattfaut, R. (2017) Internet adoption by the elderly: employing IS technology acceptance theories for understanding the age-related digital divide, *European Journal of Information Systems*, 23(6), pp. 708-726. doi: 10.1057/ejis.2013.19.

Norges Bank (2020) *Finansiell Infrastruktur 2020*. Available at: https://static.norges-bank.no/contentassets/8971421ae47b47a1be6576f17a415f5c/fi_finansiellinfrastruktur2020.pdf?v=05/19/2020110355&ft=.pdf (Accessed: 28 June 2020).

NTT DoCoMo (2003) *DoCoMo's Newest 505i Handset Features Fingerprint Authentication*. Available at: https://www.nttdocomo.co.jp/english/info/media_center/pr/2003/000985.html (Accessed: 20 February 2020).

Nyquist, J. (2019) *Slik har iPhone endret livene våre*. Available at: https://www.online.no/apple/iphone-innovasjon (Accessed: 21 February 2020).

Ogbanufe, O. and Kim, D. J. (2018) Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, *Decision Support Systems*, 106, pp. 1-14. doi: 10.1016/j.dss.2017.11.003.

Padilla-Meléndez, A., del Aguila-Obra, A. R. and Garrido-Moreno, A. (2013) Perceived playfulness, gender differences and technology acceptance model in a blended learning scenario, *Computers & Education*, 63, pp. 306-317. doi: 10.1016/j.compedu.2012.12.014.

Pallant, J. (2016) *SPSS Survival Manual*. 6 edn. Maidenhead: Open University Press/McGraw-Hill.

Parry, S. (n.d.) Fit Indices commonly reported for CFA and SEM: Cornell University Consulting Unit. Available at: https://www.cscu.cornell.edu/news/Handouts/SEM_fit.pdf.

Petersen, J. (2019) The complexity of consent and privacy in biometrics – worldwide, *Biometric Technology Today*, 2019(8), pp. 5-7. doi: 10.1016/s0969-4765(19)30113-4.

Privacytrust (2018) *Whats the real purpose of the GDPR*. Available at: https://www.privacytrust.com/gdpr/whats-the-real-purpose-of-the-gdpr.html (Accessed: 8 May 2020).

PwC (2016) *FinTech Q&A*. Available at: https://www.pwc.com/us/en/financial-services/publications/viewpoints/assets/pwc-fsi-what-is-fintech.pdf (Accessed: 27 June 2020).

PwC (n.d.) *Tilit i en digital finansverden*. Available at: https://www.pwc.no/no/pwc-aktuelt/tillitsstyring-i-en-digital-verden.html (Accessed: 26 June 2020).

Rahi, S., Ghani, M. A. and Alnaser, F. M. (2017) Predicting customer's intentions to use internet banking: the role of technology acceptance model (TAM) in e-banking, *Management Science Letters*, pp. 513-524. doi: 10.5267/j.msl.2017.8.004.

Rahi, S. *et al.* (2019) Integration of UTAUT model in internet banking adoption context, *Journal of Research in Interactive Marketing*, 13(3), pp. 411-435. doi: 10.1108/jrim-02-2018-0032.

Rainie, L. and Anderson, J. (2017) *The Fate of Online Trust in the Next Decade*. Available at: https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2017/08/PI_2017.08.10_onlineTrustNextDecade_FINAL.pdf (Accessed: 2 June 2020).

Razzak, A. (2017) *The rise of Biometrics*. Available at: http://www.fintechbd.com/the-rise-of-biometrics/ (Accessed: 21 February 2020).

Regjeringen (n.d.) *The Financial Supervisory Authority (Finanstilsynet)*. Available at: https://www.regjeringen.no/en/dep/fin/about-the-ministry/subordinateagencies/the-financial-supervisory-authority/id270404/ (Accessed: June 24 2020).

Sharma, G. (2016) *«Why China is the FinTech Capital of the World?» - 50 Point Summary*. Available at: https://medium.com/@gaurav.sharma/why-china-is-the-fintech-capital-of-the-world-50-points-summary-6f3a66159196 (Accessed: 8 June 2020).

Sharma, S. K. (2017) Integrating cognitive antecedents into TAM to explain mobile banking behavioral intention: A SEM-neural network modeling, *Information Systems Frontiers*, 21(4), pp. 815-827. doi: 10.1007/s10796-017-9775-x.

Smartpls (n.d) *How to interpret excess kurtosis and skewness*. Available at: https://www.smartpls.com/documentation/functionalities/excess-kurtosis-and-skewness (Accessed: 3 June 2020).

Solbak, V. (2019) *"Folket" har talt: teknologi er vanskelig*. Available at: https://www.eplehjelp.no/folket-har-talt-teknologi-er-vanskelig/ (Accessed: 20 June 2020).

SSB (n.d) *Fakta om Internett og Mobil*. Available at: https://www.ssb.no/teknologi-og-innovasjon/faktaside (Accessed: 15 May 2020).

Statistics Solutions (n.d) *Cronbach's Alpha*. Available at: https://www.statisticssolutions.com/cronbachs-alpha/ (Accessed: 28 June 2020).

Stoll, J. (2020) *Monthly Vipps app DAU in Norway 2019-2020*. Available at: https://www.statista.com/statistics/1098029/monthly-vipps-app-dau-in-norway/ (Accessed: 25 June 2020).

Stranden, A. L. (2017) *Eldre som blir svindlet, regner og husker dårligere enn andre*. Available at: https://forskning.no/markedsforing-forbruk/eldre-som-blir-svindlet-regner-og-husker-darligere-enn-andre/351443 (Accessed: 21 June 2020).

Surendran, P. (2012) Technology Acceptance Model: A Survey of Literature, *International journal of Business and Social Research*, 2(4), pp. 175-178. doi: 10.18533/ijbsr.v2i4.161.

Szajna, B. (1996) Empirical Evaluation of the Revised Technology Acceptance Model, *Management Science*, 42(1), pp. 85-92. Available at: http://www.jstor.com/stable/2633017 (Accessed: 20 June 2020).

Sønsteng, S. (2020) *Har ikke åpnet den digitale lommeboken*. Available at: https://www.elektronikkbransjen.no/artikler/har-ikke-apnet-den-digitale-lommeboken/488402 (Accessed: 26 June 2020).

Tavakol, M. and Dennick, R. (2011) Making sense of Cronbach's α, *International Journal of Medical Education*, pp. 53-55. doi: 10.5116/ijme.4dfb.8dfd.

Thakkar, D. (n.d.) *Biometric Performance Metrics Can Help You Select the Right Biometric Solution*. Available at: https://www.bayometric.com/biometric-performance-metrics-select-right-solution/ (Accessed: 22 March 2020).

The Future Laboratory (2019) *Fintech Futures Report*. The Future Laboratory.

Trader, J. (n.d) *The impact of Biometrics in banking*. Available at: http://www.m2sys.com/blog/financial-services/impact-biometrics-banking/ (Accessed: 24 February 2020).

Utdanningsforbundet (2017) *Om sammenhengen mellom utdanning og tilit*. Seksjon for samfunn og analyse i avdeling for profesjonspolitikk. Available at: https://www.utdanningsforbundet.no/globalassets/var-politikk/publikasjoner/temanotat/2017/temanotat_04.2017.pdf (Accessed: 2 June 2020).

Utheim, E. B. (2013) *Ola og Kari grepet av teknologiangst*. Available at: https://e24.no/teknologi/i/LA3n7J/ola-og-kari-grepet-av-teknologiangst (Accessed: 21 June 2020).

Vahdat, A. *et al.* (2020) Would you like to shop via mobile app technology? The technology acceptance model, social factors and purchase intention, *Australasian Marketing Journal (AMJ)*. doi: 10.1016/j.ausmj.2020.01.002.

Venkatesh, V. *et al.* (2003) User Acceptance of Information Technology: Toward a Unified View, *MIS Quarterly*, 27(3), pp. 425-478. doi: 10.2307/30036540.

Waterson, L. S. (n.d) *Application of Biometric Technology in different sectors*. Available at: http://www.m2sys.com/blog/biometric-technology/application-of-biometric-technology-in-different-sectors/ (Accessed: 21 February 2020 2020).

Wei, Z., Zhao, Z. and Zheng, Y. (2019) Following the Majority: Social Influence in Trusting Behavior, *Front Neurosci*, 13, pp. 8. doi: 10.3389/fnins.2019.00089.

Welch, C. (2017) *Amazon's Alexa can now recognize different voices and give personalized responses*. Available at: https://www.theverge.com/circuitbreaker/2017/10/11/16460120/amazon-echo-multi-user-voice-new-feature (Accessed: 24 June 2020).

Winck, B. (2020) *The 5 most valuable US tech companies are now worth more than $5 trillion after Alphabet's record close*. Available at: https://markets.businessinsider.com/news/stocks/most-valuable-tech-companies-total-worth-trillions-alphabet-stock-record-2020-1-1028826533 (Accessed: 24 June 2020).

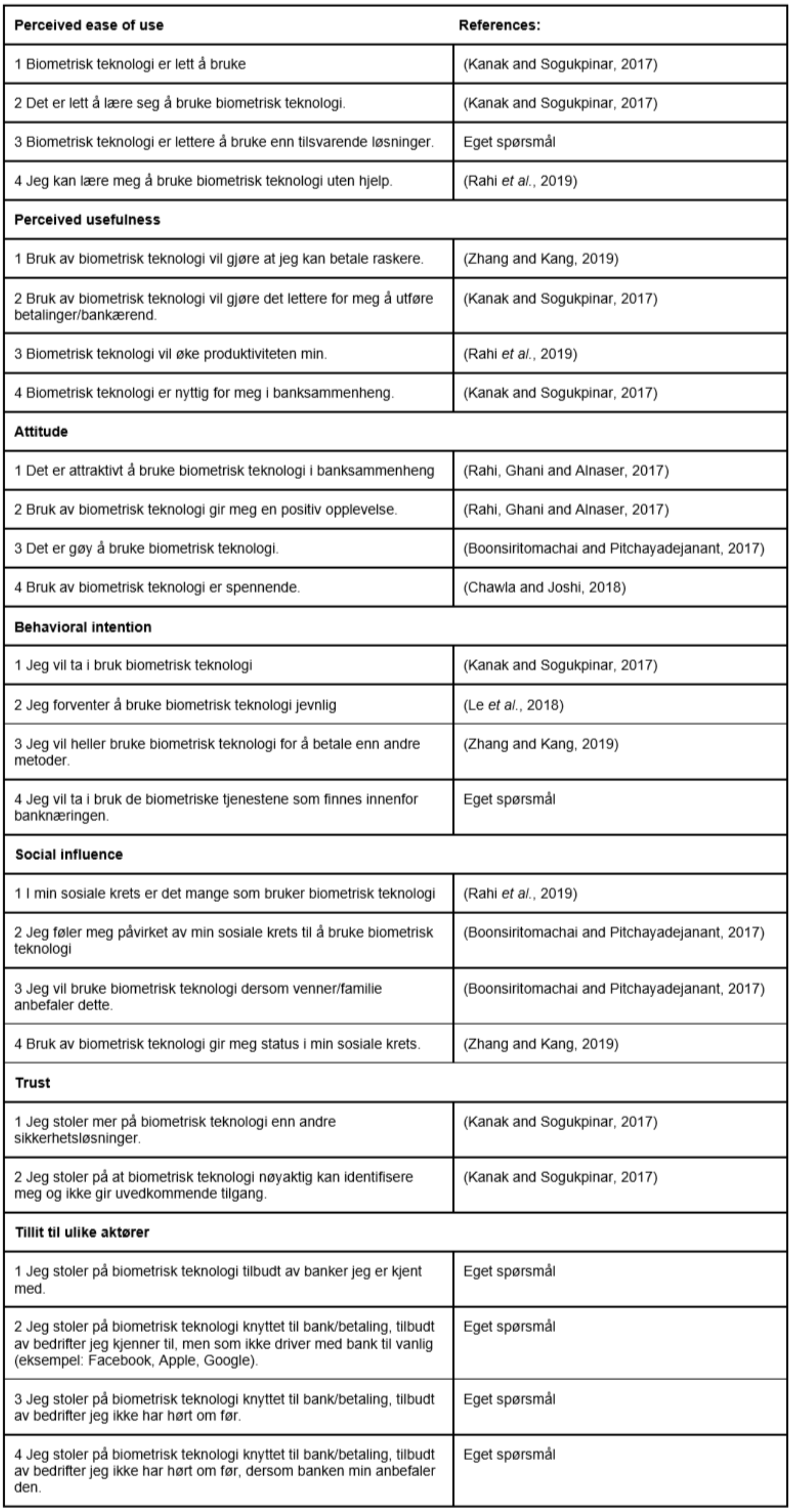
Winther, M. W. (2019) *PSD2 is finally incorporated into the EEA-agreement*. Available at: https://svw.no/aktuelt/aktuelt/2019/juni/psd2-is-finally-incorporated-into-the-eea-agreement/ (Accessed: 21 February 2020).

World Economic Forum (2019) *Global Gender Gap Report 2020*.

Zhang, L., Nyheim, P. and S. Mattila, A. (2014) The effect of power and gender on technology acceptance, *Journal of Hospitality and Tourism Technology*, 5(3), pp. 299-314. doi: 10.1108/jhtt-03-2014-0008.

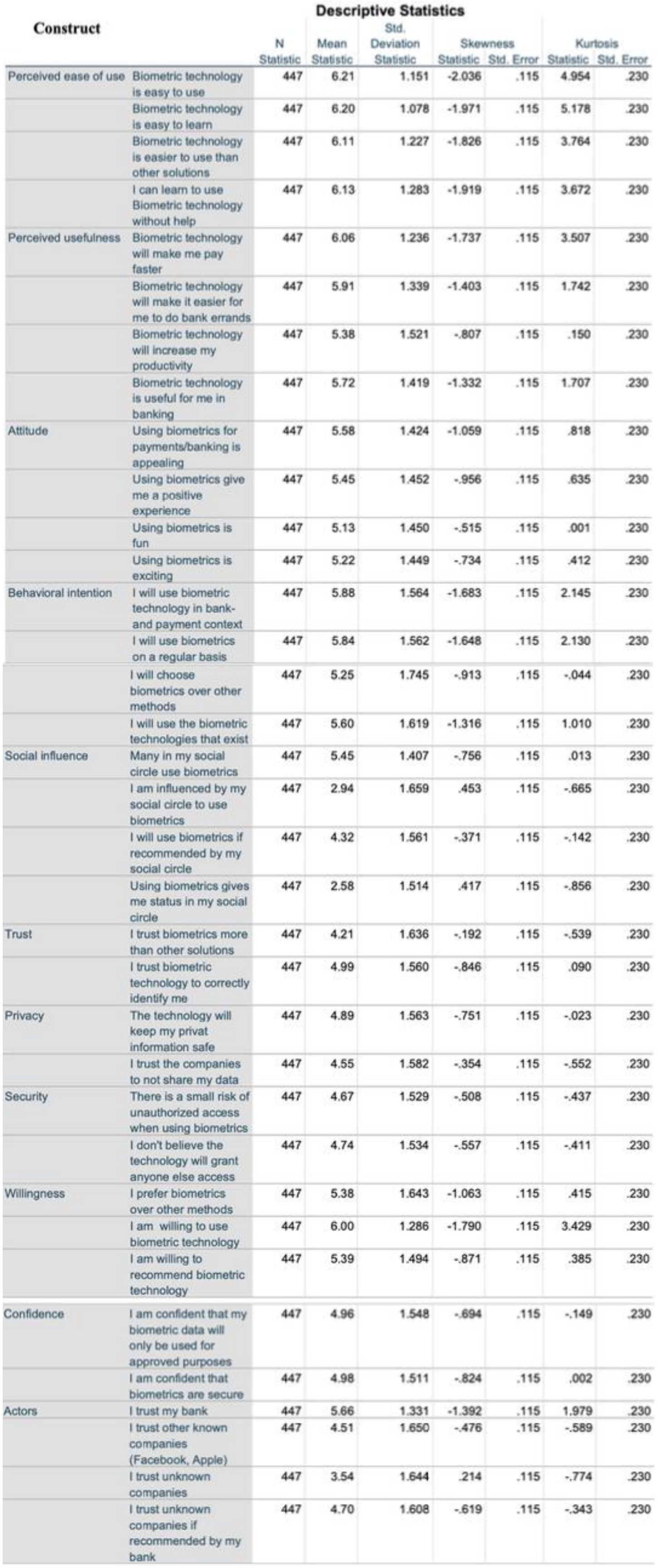
Zhang, W. K. and Kang, M. J. (2019) Factors Affecting the Use of Facial-Recognition Payment: An Example of Chinese Consumers, *IEEE Access*, 7, pp. 154360-154374. doi: 10.1109/access.2019.2927705.

Appendix A – questionnaire with references



Perceived ease of use	**References:**
1 Biometrisk teknologi er lett å bruke	(Kanak and Sogukpinar, 2017)
2 Det er lett å lære seg å bruke biometrisk teknologi.	(Kanak and Sogukpinar, 2017)
3 Biometrisk teknologi er lettere å bruke enn tilsvarende løsninger.	Eget spørsmål
4 Jeg kan lære meg å bruke biometrisk teknologi uten hjelp.	(Rahi *et al.*, 2019)
Perceived usefulness	
1 Bruk av biometrisk teknologi vil gjøre at jeg kan betale raskere.	(Zhang and Kang, 2019)
2 Bruk av biometrisk teknologi vil gjøre det lettere for meg å utføre betalinger/bankærend.	(Kanak and Sogukpinar, 2017)
3 Biometrisk teknologi vil øke produktiviteten min.	(Rahi *et al.*, 2019)
4 Biometrisk teknologi er nyttig for meg i banksammenheng.	(Kanak and Sogukpinar, 2017)
Attitude	
1 Det er attraktivt å bruke biometrisk teknologi i banksammenheng	(Rahi, Ghani and Alnaser, 2017)
2 Bruk av biometrisk teknologi gir meg en positiv opplevelse.	(Rahi, Ghani and Alnaser, 2017)
3 Det er gøy å bruke biometrisk teknologi.	(Boonsiritomachai and Pitchayadejanant, 2017)
4 Bruk av biometrisk teknologi er spennende.	(Chawla and Joshi, 2018)
Behavioral intention	
1 Jeg vil ta i bruk biometrisk teknologi	(Kanak and Sogukpinar, 2017)
2 Jeg forventer å bruke biometrisk teknologi jevnlig	(Le *et al.*, 2018)
3 Jeg vil heller bruke biometrisk teknologi for å betale enn andre metoder.	(Zhang and Kang, 2019)
4 Jeg vil ta i bruk de biometriske tjenestene som finnes innenfor banknæringen.	Eget spørsmål
Social influence	
1 I min sosiale krets er det mange som bruker biometrisk teknologi	(Rahi *et al.*, 2019)
2 Jeg føler meg påvirket av min sosiale krets til å bruke biometrisk teknologi	(Boonsiritomachai and Pitchayadejanant, 2017)
3 Jeg vil bruke biometrisk teknologi dersom venner/familie anbefaler dette.	(Boonsiritomachai and Pitchayadejanant, 2017)
4 Bruk av biometrisk teknologi gir meg status i min sosiale krets.	(Zhang and Kang, 2019)
Trust	
1 Jeg stoler mer på biometrisk teknologi enn andre sikkerhetsløsninger.	(Kanak and Sogukpinar, 2017)
2 Jeg stoler på at biometrisk teknologi nøyaktig kan identifisere meg og ikke gir uvedkommende tilgang.	(Kanak and Sogukpinar, 2017)
Tillit til ulike aktører	
1 Jeg stoler på biometrisk teknologi tilbudt av banker jeg er kjent med.	Eget spørsmål
2 Jeg stoler på biometrisk teknologi knyttet til bank/betaling, tilbudt av bedrifter jeg kjenner til, men som ikke driver med bank til vanlig (eksempel: Facebook, Apple, Google).	Eget spørsmål
3 Jeg stoler på biometrisk teknologi knyttet til bank/betaling, tilbudt av bedrifter jeg ikke har hørt om før.	Eget spørsmål
4 Jeg stoler på biometrisk teknologi knyttet til bank/betaling, tilbudt av bedrifter jeg ikke har hørt om før, dersom banken min anbefaler den.	Eget spørsmål

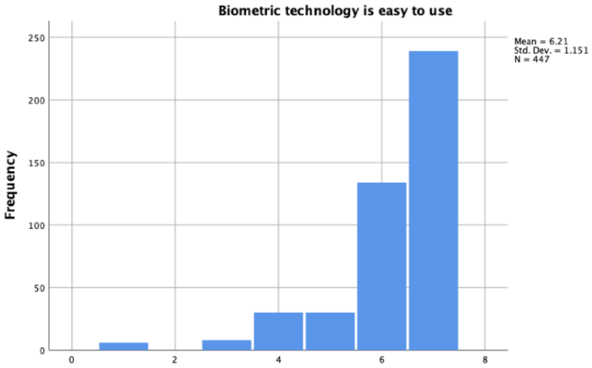
Appendix B – descriptive statistics

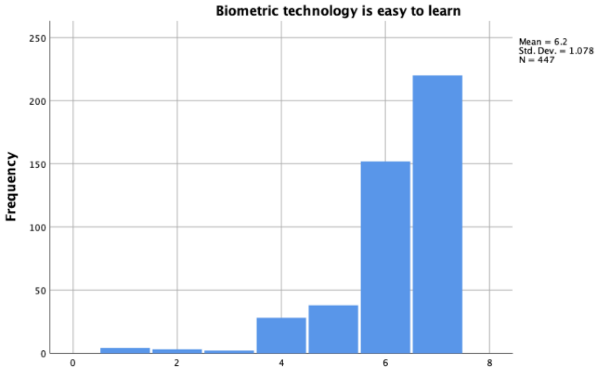


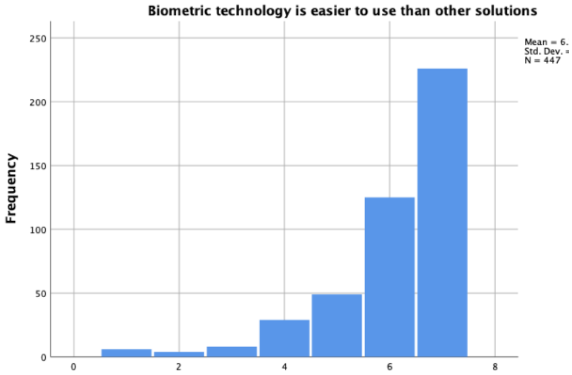
Descriptive Statistics

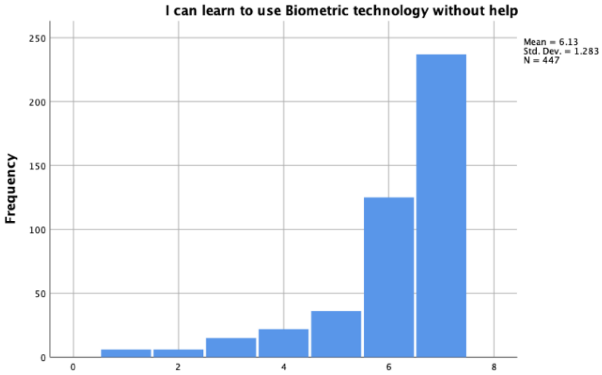
Construct		N	Mean	Std. Deviation	Skewness		Kurtosis	
		Statistic	Statistic	Statistic	Statistic	Std. Error	Statistic	Std. Error
Perceived ease of use	Biometric technology is easy to use	447	6.21	1.151	-2.036	.115	4.954	.230
	Biometric technology is easy to learn	447	6.20	1.078	-1.971	.115	5.178	.230
	Biometric technology is easier to use than other solutions	447	6.11	1.227	-1.826	.115	3.764	.230
	I can learn to use Biometric technology without help	447	6.13	1.283	-1.919	.115	3.672	.230
Perceived usefulness	Biometric technology will make me pay faster	447	6.06	1.236	-1.737	.115	3.507	.230
	Biometric technology will make it easier for me to do bank errands	447	5.91	1.339	-1.403	.115	1.742	.230
	Biometric technology will increase my productivity	447	5.38	1.521	-.807	.115	.150	.230
	Biometric technology is useful for me in banking	447	5.72	1.419	-1.332	.115	1.707	.230
Attitude	Using biometrics for payments/banking is appealing	447	5.58	1.424	-1.059	.115	.818	.230
	Using biometrics give me a positive experience	447	5.45	1.452	-.956	.115	.635	.230
	Using biometrics is fun	447	5.13	1.450	-.515	.115	.001	.230
	Using biometrics is exciting	447	5.22	1.449	-.734	.115	.412	.230
Behavioral intention	I will use biometric technology in bank- and payment context	447	5.88	1.564	-1.683	.115	2.145	.230
	I will use biometrics on a regular basis	447	5.84	1.562	-1.648	.115	2.130	.230
	I will choose biometrics over other methods	447	5.25	1.745	-.913	.115	-.044	.230
	I will use the biometric technologies that exist	447	5.60	1.619	-1.316	.115	1.010	.230
Social influence	Many in my social circle use biometrics	447	5.45	1.407	-.756	.115	.013	.230
	I am influenced by my social circle to use biometrics	447	2.94	1.659	.453	.115	-.665	.230
	I will use biometrics if recommended by my social circle	447	4.32	1.561	-.371	.115	-.142	.230
	Using biometrics gives me status in my social circle	447	2.58	1.514	.417	.115	-.856	.230
Trust	I trust biometrics more than other solutions	447	4.21	1.636	-.192	.115	-.539	.230
	I trust biometric technology to correctly identify me	447	4.99	1.560	-.846	.115	.090	.230
Privacy	The technology will keep my privat information safe	447	4.89	1.563	-.751	.115	-.023	.230
	I trust the companies to not share my data	447	4.55	1.582	-.354	.115	-.552	.230
Security	There is a small risk of unauthorized access when using biometrics	447	4.67	1.529	-.508	.115	-.437	.230
	I don't believe the technology will grant anyone else access	447	4.74	1.534	-.557	.115	-.411	.230
Willingness	I prefer biometrics over other methods	447	5.38	1.643	-1.063	.115	.415	.230
	I am willing to use biometric technology	447	6.00	1.286	-1.790	.115	3.429	.230
	I am willing to recommend biometric technology	447	5.39	1.494	-.871	.115	.385	.230
Confidence	I am confident that my biometric data will only be used for approved purposes	447	4.96	1.548	-.694	.115	-.149	.230
	I am confident that biometrics are secure	447	4.98	1.511	-.824	.115	.002	.230
Actors	I trust my bank	447	5.66	1.331	-1.392	.115	1.979	.230
	I trust other known companies (Facebook, Apple)	447	4.51	1.650	-.476	.115	-.589	.230
	I trust unknown companies	447	3.54	1.644	.214	.115	-.774	.230
	I trust unknown companies if recommended by my bank	447	4.70	1.608	-.619	.115	-.343	.230

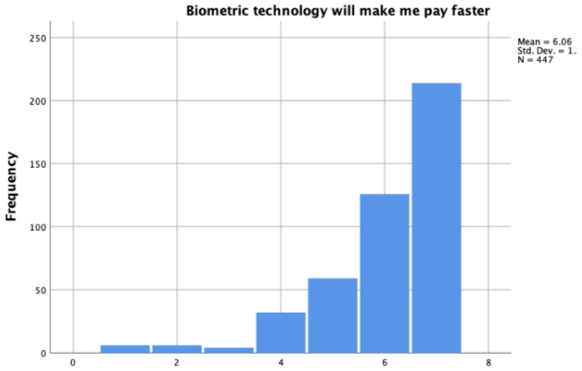
Appendix C - histograms

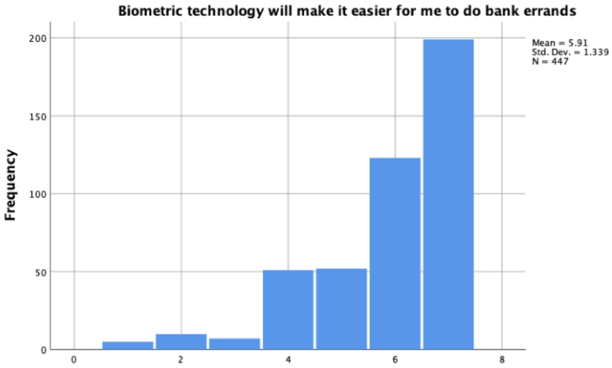


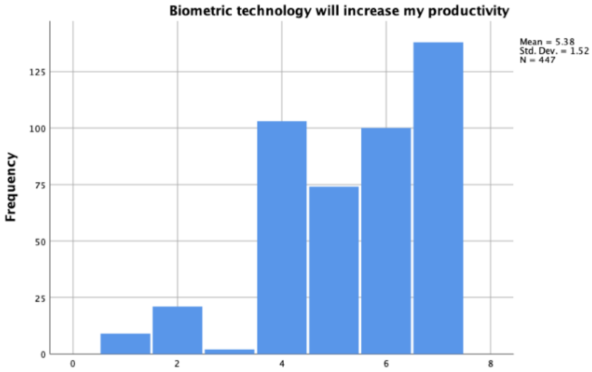


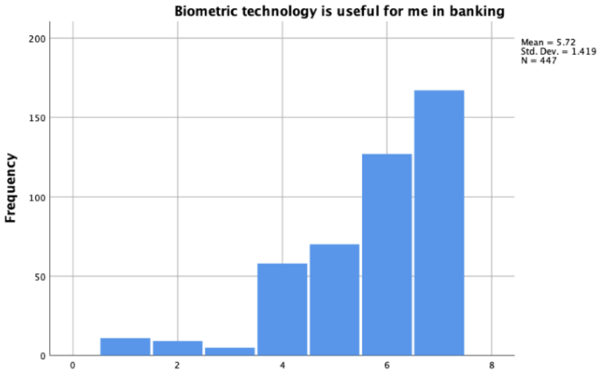


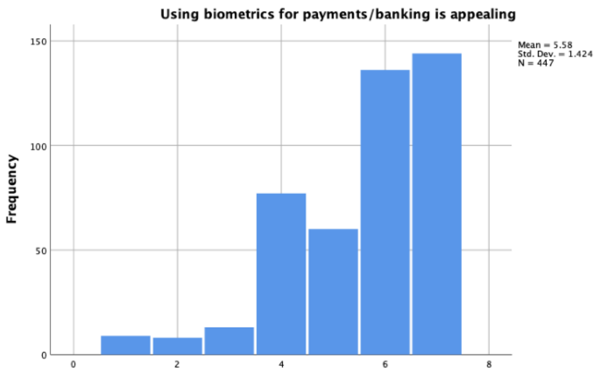


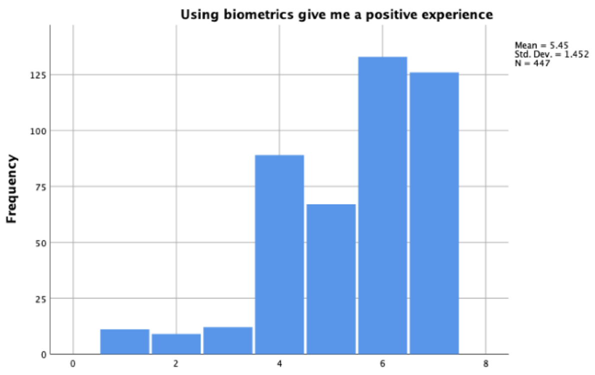


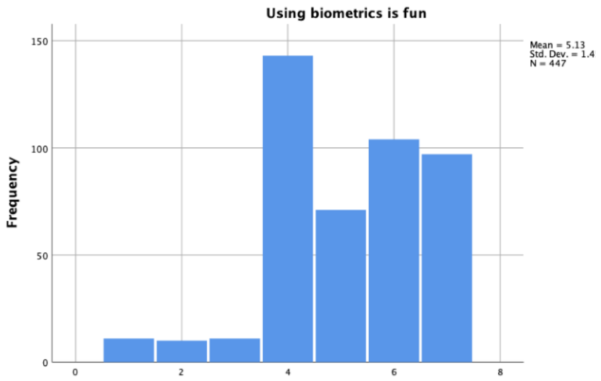


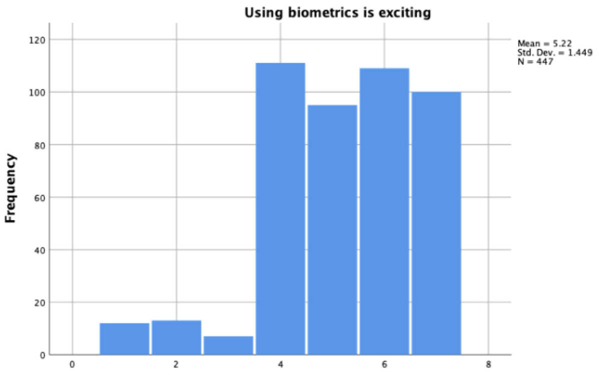


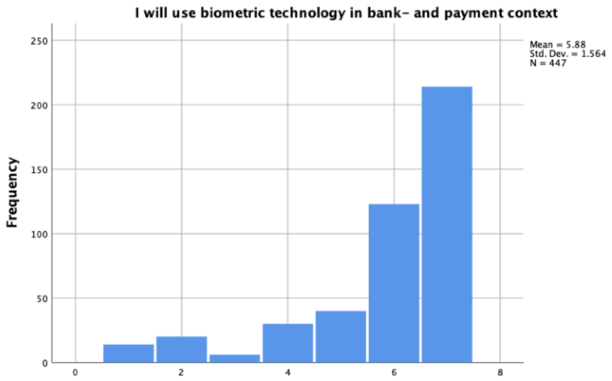


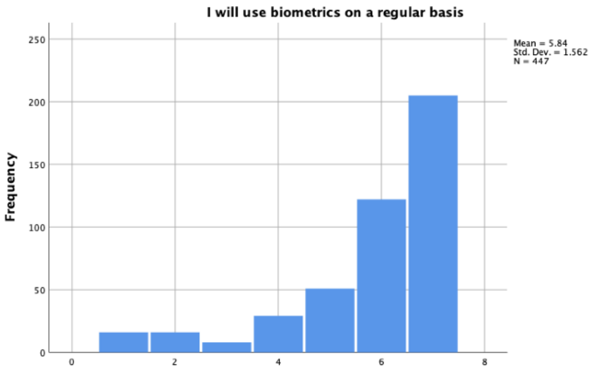

Using biometrics for payments/banking is appealing
Frequency
0
50
100
150
0
2
4
6
8
Mean = 5.58
Std. Dev. = 1.424
N = 447

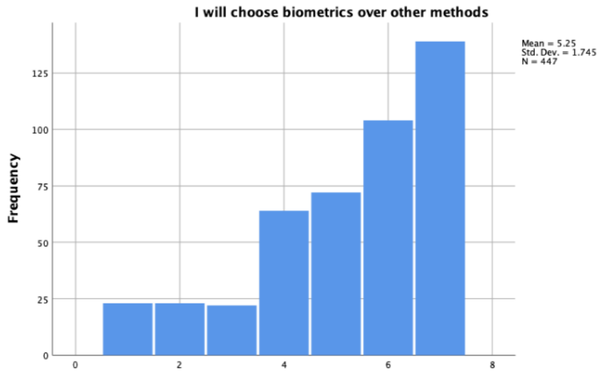

Using biometrics give me a positive experience
Frequency
0
25
50
75
100
125
0
2
4
6
8
Mean = 5.45
Std. Dev. = 1.452
N = 447

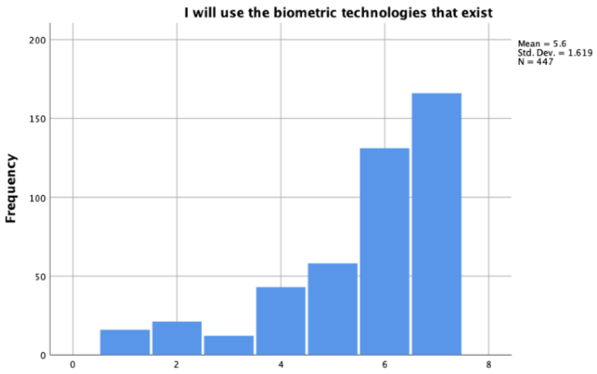

Using biometrics is fun
Frequency
0
50
100
150
0
2
4
6
8
Mean = 5.13
Std. Dev. = 1.4
N = 447

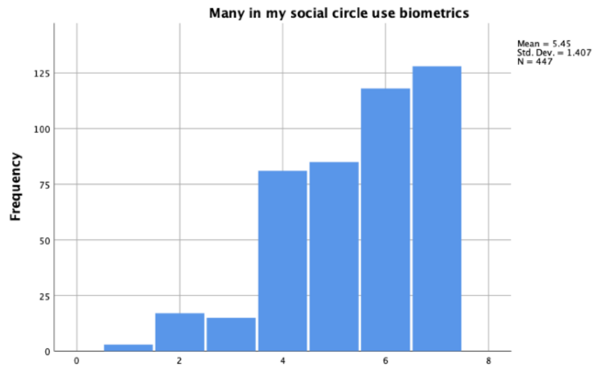

Using biometrics is exciting
Frequency
0
20
40
60
80
100
120
0
2
4
6
8
Mean = 5.22
Std. Dev. = 1.449
N = 447

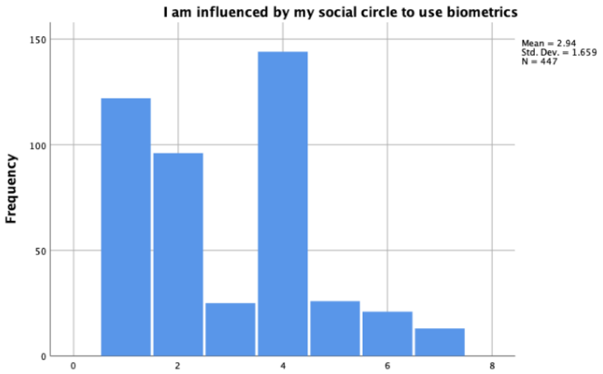

I will use biometric technology in bank- and payment context
Frequency
0
50
100
150
200
250
0
2
4
6
8
Mean = 5.88
Std. Dev. = 1.564
N = 447

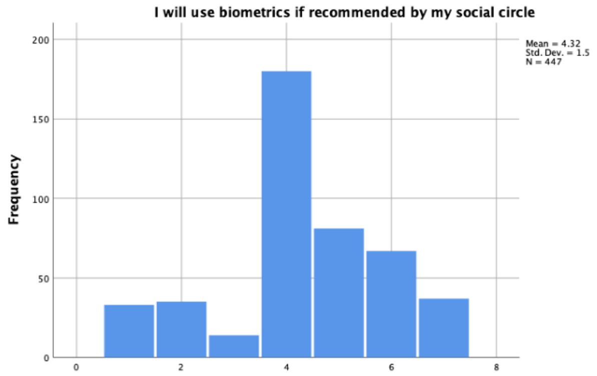

I will use biometrics on a regular basis
Frequency
0
50
100
150
200
250
0
2
4
6
8
Mean = 5.84
Std. Dev. = 1.562
N = 447

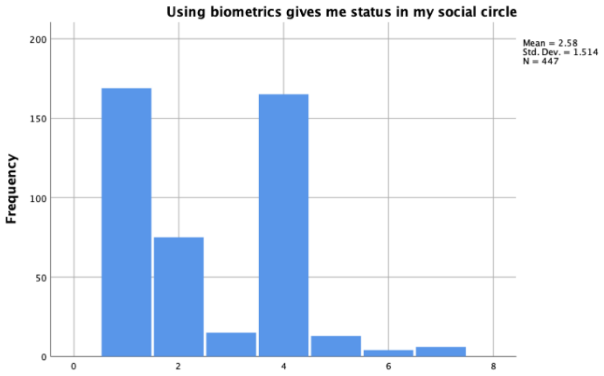

I will choose biometrics over other methods
Frequency
0
25
50
75
100
125
0
2
4
6
8
Mean = 5.25
Std. Dev. = 1.745
N = 447

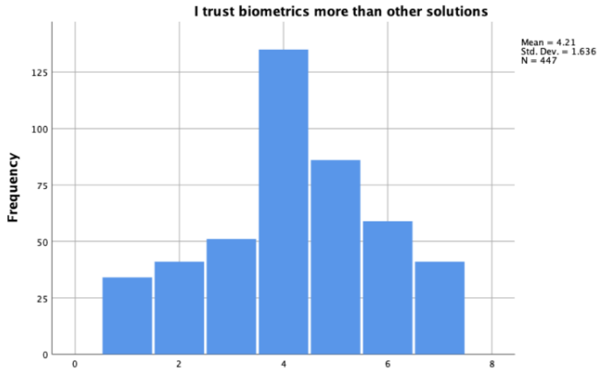

I will use the biometric technologies that exist
Frequency
0
50
100
150
200
0
2
4
6
8
Mean = 5.6
Std. Dev. = 1.619
N = 447

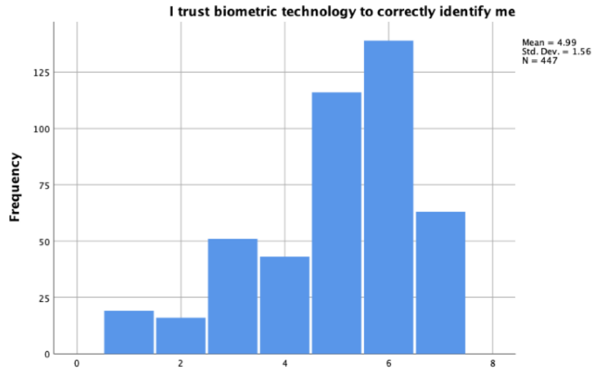

Many in my social circle use biometrics
Mean = 5.45
Std. Dev. = 1.407
N = 447
Frequency
0
25
50
75
100
125
0
2
4
6
8


I am influenced by my social circle to use biometrics
Mean = 2.94
Std. Dev. = 1.659
N = 447
Frequency
0
50
100
150
0
2
4
6
8


I will use biometrics if recommended by my social circle
Mean = 4.32
Std. Dev. = 1.5
N = 447
Frequency
0
50
100
150
200
0
2
4
6
8

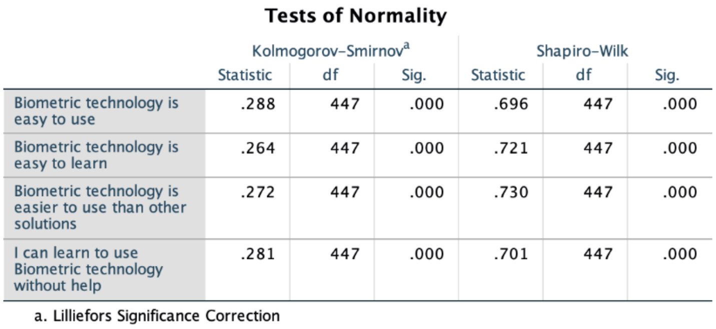

Using biometrics gives me status in my social circle
Mean = 2.58
Std. Dev. = 1.514
N = 447
Frequency
0
50
100
150
200
0
2
4
6
8


I trust biometrics more than other solutions
Mean = 4.21
Std. Dev. = 1.636
N = 447
Frequency
0
25
50
75
100
125
0
2
4
6
8


I trust biometric technology to correctly identify me
Mean = 4.99
Std. Dev. = 1.56
N = 447
Frequency
0
25
50
75
100
125
0
2
4
6
8

Appendix D – test of normality

Perceived Ease of Use:

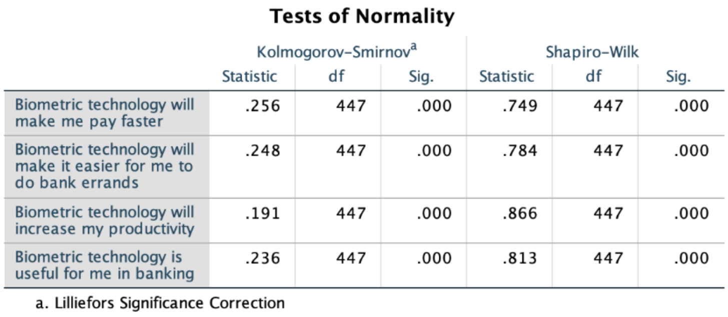


Tests of Normality

	Kolmogorov–Smirnov[a]			Shapiro–Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Biometric technology is easy to use	.288	447	.000	.696	447	.000
Biometric technology is easy to learn	.264	447	.000	.721	447	.000
Biometric technology is easier to use than other solutions	.272	447	.000	.730	447	.000
I can learn to use Biometric technology without help	.281	447	.000	.701	447	.000

a. Lilliefors Significance Correction

Perceived Usefulness:

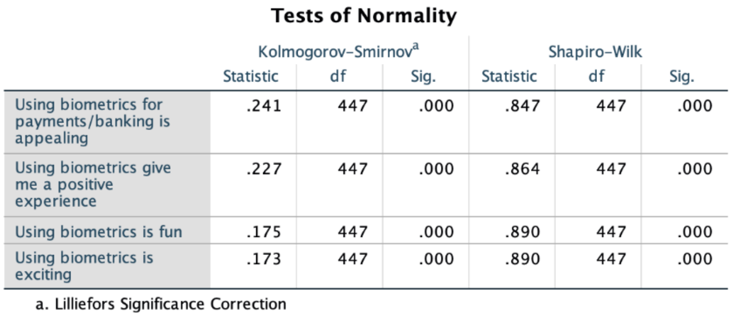


Tests of Normality

	Kolmogorov–Smirnov[a]			Shapiro–Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Biometric technology will make me pay faster	.256	447	.000	.749	447	.000
Biometric technology will make it easier for me to do bank errands	.248	447	.000	.784	447	.000
Biometric technology will increase my productivity	.191	447	.000	.866	447	.000
Biometric technology is useful for me in banking	.236	447	.000	.813	447	.000

a. Lilliefors Significance Correction

Attitude:

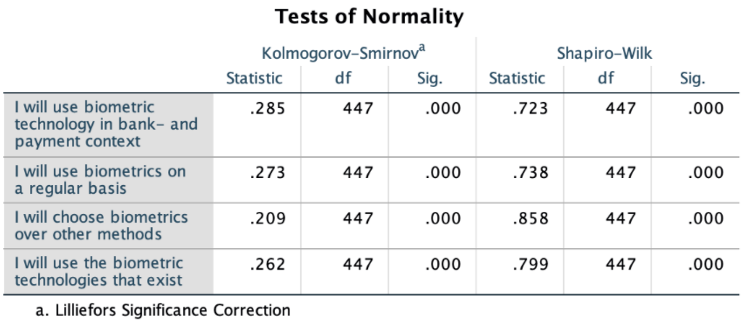


Tests of Normality

	Kolmogorov–Smirnov[a]			Shapiro–Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Using biometrics for payments/banking is appealing	.241	447	.000	.847	447	.000
Using biometrics give me a positive experience	.227	447	.000	.864	447	.000
Using biometrics is fun	.175	447	.000	.890	447	.000
Using biometrics is exciting	.173	447	.000	.890	447	.000

a. Lilliefors Significance Correction

BI:

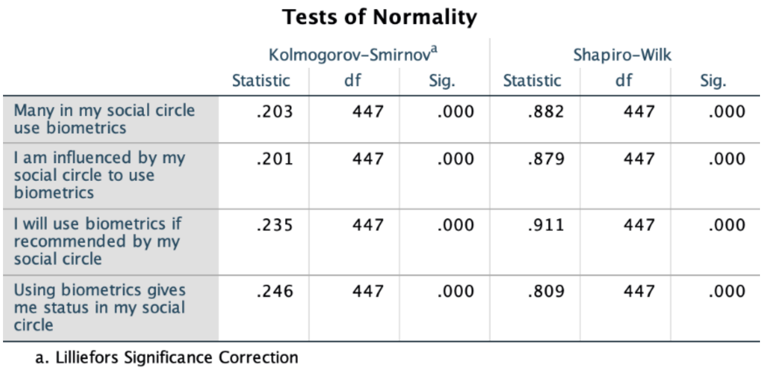


Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
I will use biometric technology in bank- and payment context	.285	447	.000	.723	447	.000
I will use biometrics on a regular basis	.273	447	.000	.738	447	.000
I will choose biometrics over other methods	.209	447	.000	.858	447	.000
I will use the biometric technologies that exist	.262	447	.000	.799	447	.000

a. Lilliefors Significance Correction

SI:

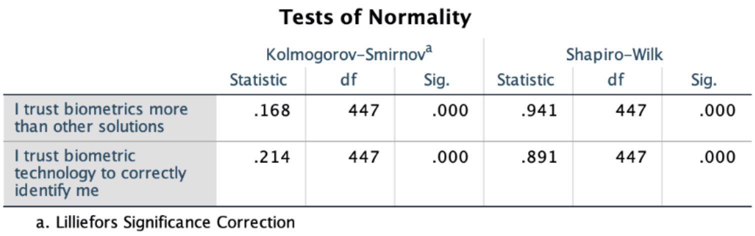


Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Many in my social circle use biometrics	.203	447	.000	.882	447	.000
I am influenced by my social circle to use biometrics	.201	447	.000	.879	447	.000
I will use biometrics if recommended by my social circle	.235	447	.000	.911	447	.000
Using biometrics gives me status in my social circle	.246	447	.000	.809	447	.000

a. Lilliefors Significance Correction

Trust:

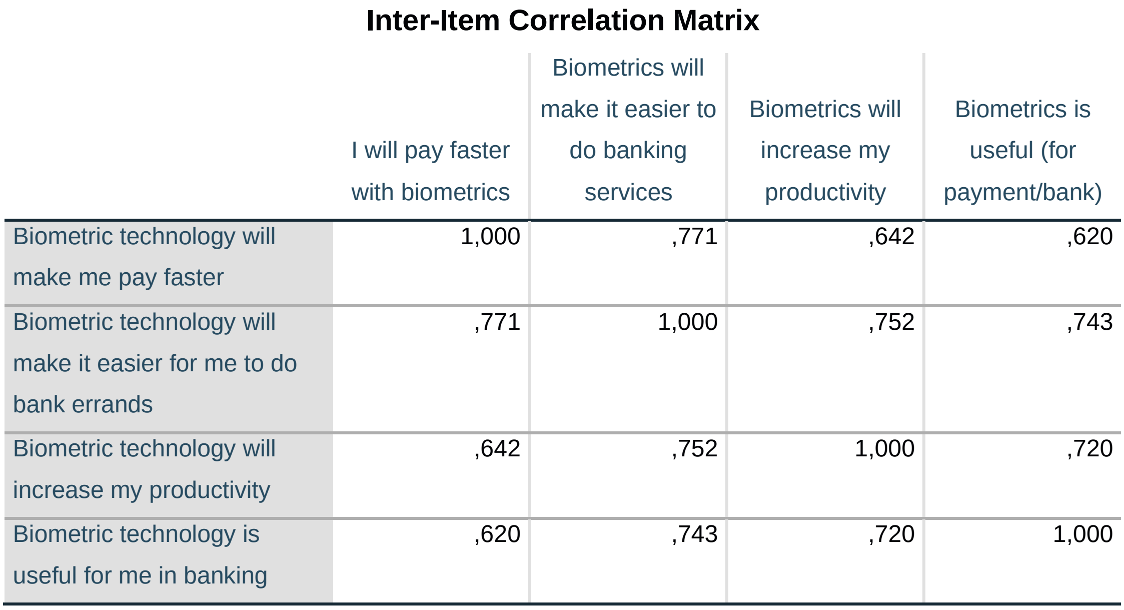


Tests of Normality

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
I trust biometrics more than other solutions	.168	447	.000	.941	447	.000
I trust biometric technology to correctly identify me	.214	447	.000	.891	447	.000

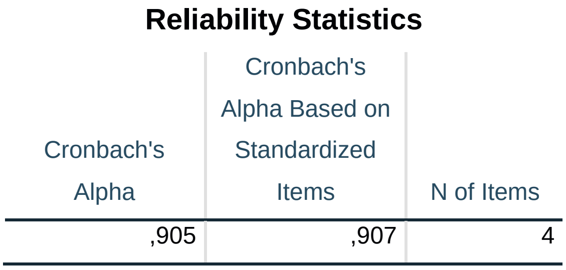
a. Lilliefors Significance Correction

Appendix E - reliability analysis for PU



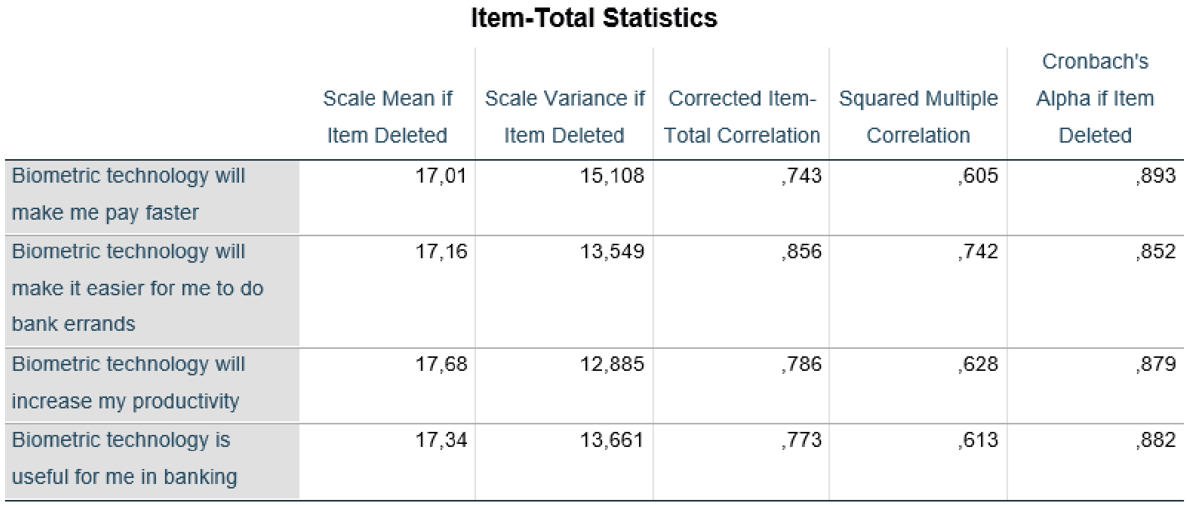
Inter-Item Correlation Matrix

	I will pay faster with biometrics	Biometrics will make it easier to do banking services	Biometrics will increase my productivity	Biometrics is useful (for payment/bank)
Biometric technology will make me pay faster	1,000	,771	,642	,620
Biometric technology will make it easier for me to do bank errands	,771	1,000	,752	,743
Biometric technology will increase my productivity	,642	,752	1,000	,720
Biometric technology is useful for me in banking	,620	,743	,720	1,000



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,905	,907	4



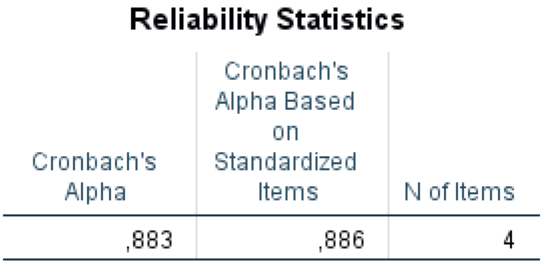
Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Biometric technology will make me pay faster	17,01	15,108	,743	,605	,893
Biometric technology will make it easier for me to do bank errands	17,16	13,549	,856	,742	,852
Biometric technology will increase my productivity	17,68	12,885	,786	,628	,879
Biometric technology is useful for me in banking	17,34	13,661	,773	,613	,882

Appendix F – reliability analysis for PEOU

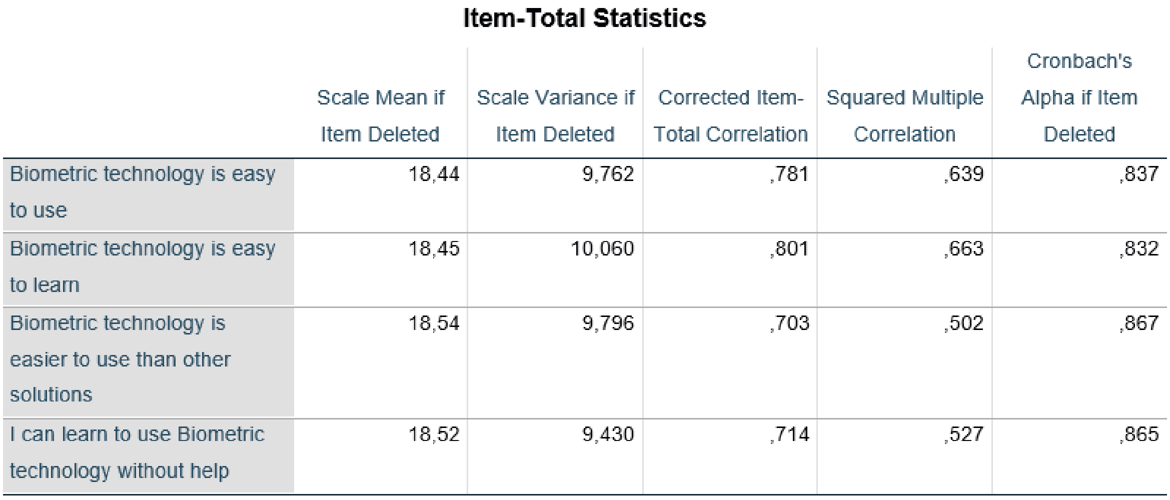
Inter-Item Correlation Matrix

	Biometrics are easy to use	Biometrics are easy to learn	Biometrics are easier to use than other solutions	I can learn to use biometrics without help
Biometric technology is easy to use	1,000	,759	,665	,628
Biometric technology is easy to learn	,759	1,000	,633	,694
Biometric technology is easier to use than other solutions	,665	,633	1,000	,588
I can learn to use Biometric technology without help	,628	,694	,588	1,000



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,883	,886	4



Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Biometric technology is easy to use	18,44	9,762	,781	,639	,837
Biometric technology is easy to learn	18,45	10,060	,801	,663	,832
Biometric technology is easier to use than other solutions	18,54	9,796	,703	,502	,867
I can learn to use Biometric technology without help	18,52	9,430	,714	,527	,865

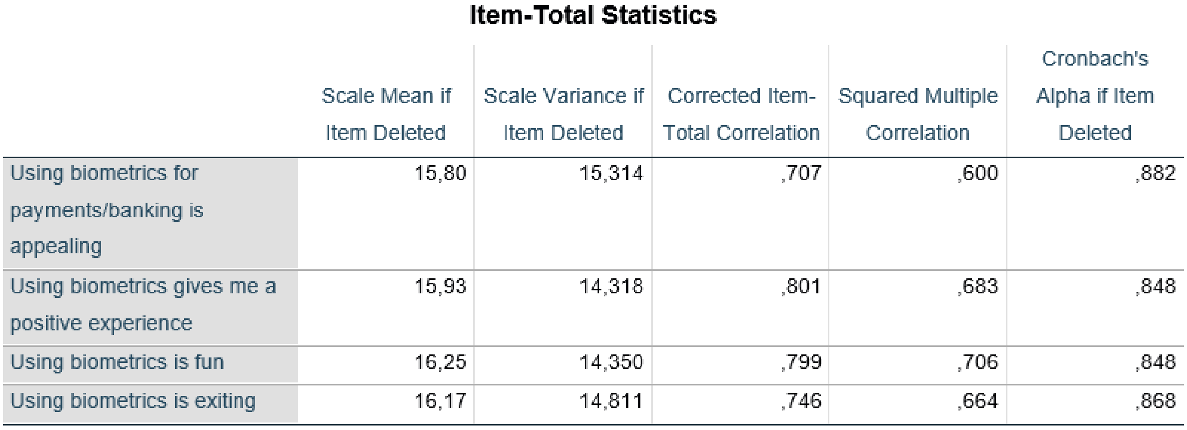
Appendix G – reliability analysis for ATT

Inter-Item Correlation Matrix

	Using biometrics for payments/banking is appealing	Biometrics give me a positive experience	Using biometrics is fun	Using biometrics is exiting
Using biometrics for payments/banking is appealing	1,000	,769	,599	,541
Using biometrics gives me a positive experience	,769	1,000	,693	,642
Using biometrics is fun	,599	,693	1,000	,806
Using biometrics is exiting	,541	,642	,806	1,000

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,893	,893	4



Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Using biometrics for payments/banking is appealing	15,80	15,314	,707	,600	,882
Using biometrics gives me a positive experience	15,93	14,318	,801	,683	,848
Using biometrics is fun	16,25	14,350	,799	,706	,848
Using biometrics is exiting	16,17	14,811	,746	,664	,868

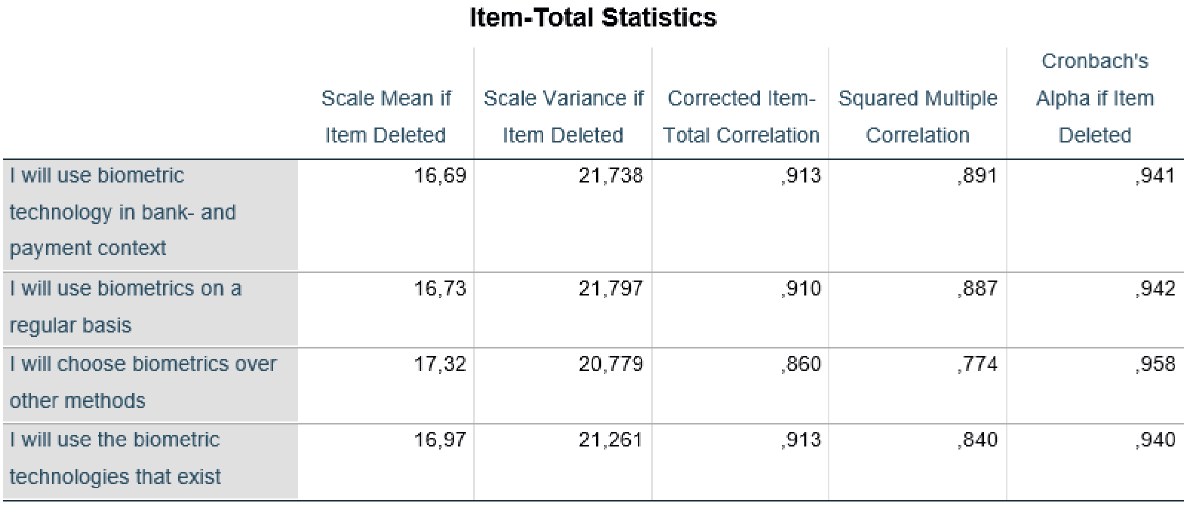
Appendix H – reliability analysis for BI

Inter-Item Correlation Matrix

	I will use biometrics	I will use biometrics on a regular basis	I will choose biometrics over other methods	I will use the biometric technologies that exist
I will use biometric technology in bank- and payment context	1,000	,936	,803	,862
I will use biometrics on a regular basis	,936	1,000	,801	,856
I will choose biometrics over other methods	,803	,801	1,000	,873
I will use the biometric technologies that exist	,862	,856	,873	1,000

Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,958	,959	4



Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
I will use biometric technology in bank- and payment context	16,69	21,738	,913	,891	,941
I will use biometrics on a regular basis	16,73	21,797	,910	,887	,942
I will choose biometrics over other methods	17,32	20,779	,860	,774	,958
I will use the biometric technologies that exist	16,97	21,261	,913	,840	,940

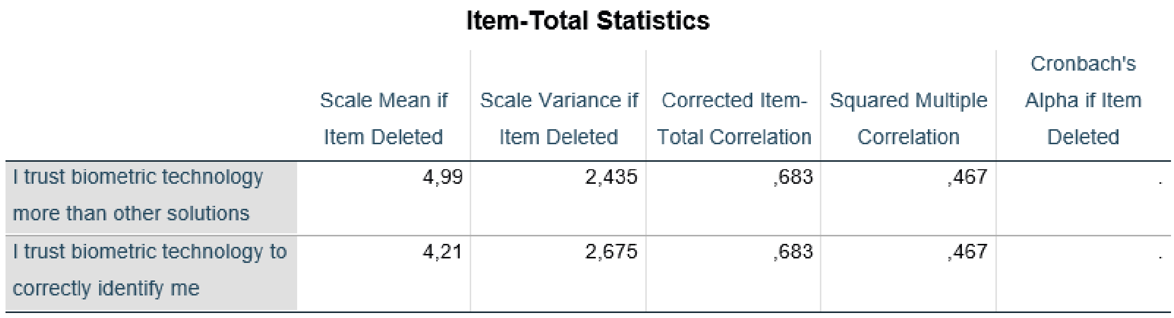
Appendix I – reliability analysis for Trust

Inter-Item Correlation Matrix

	I trust biometrics more than other solutions	I trust biometrics to identify me correctly
I trust biometric technology more than other solutions	1,000	,683
I trust biometric technology to identify me correctly	,683	1,000

Reliability Statistics

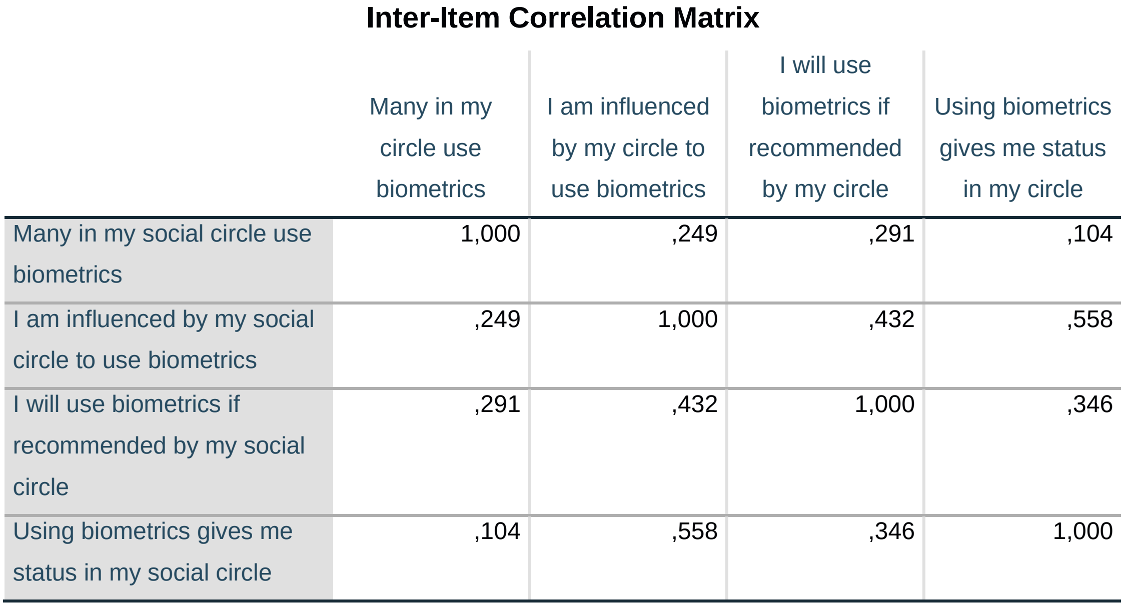
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,811	,812	2



Item-Total Statistics

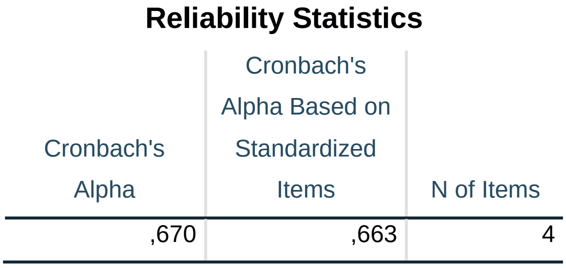
	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
I trust biometric technology more than other solutions	4,99	2,435	,683	,467	.
I trust biometric technology to correctly identify me	4,21	2,675	,683	,467	.

Appendix J – reliability analysis for SI



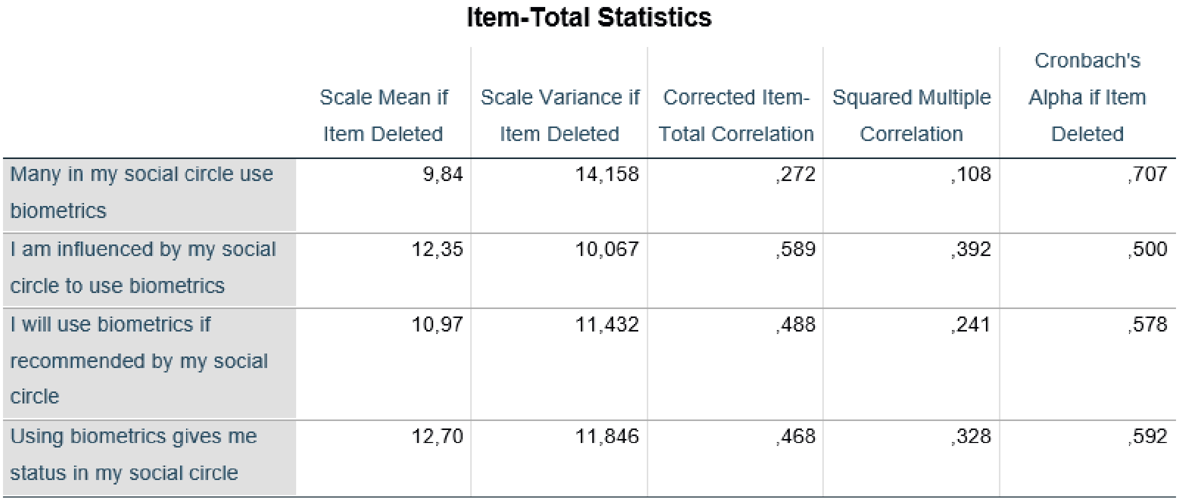
Inter-Item Correlation Matrix

	Many in my circle use biometrics	I am influenced by my circle to use biometrics	I will use biometrics if recommended by my circle	Using biometrics gives me status in my circle
Many in my social circle use biometrics	1,000	,249	,291	,104
I am influenced by my social circle to use biometrics	,249	1,000	,432	,558
I will use biometrics if recommended by my social circle	,291	,432	1,000	,346
Using biometrics gives me status in my social circle	,104	,558	,346	1,000



Reliability Statistics

Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,670	,663	4



Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
Many in my social circle use biometrics	9,84	14,158	,272	,108	,707
I am influenced by my social circle to use biometrics	12,35	10,067	,589	,392	,500
I will use biometrics if recommended by my social circle	10,97	11,432	,488	,241	,578
Using biometrics gives me status in my social circle	12,70	11,846	,468	,328	,592

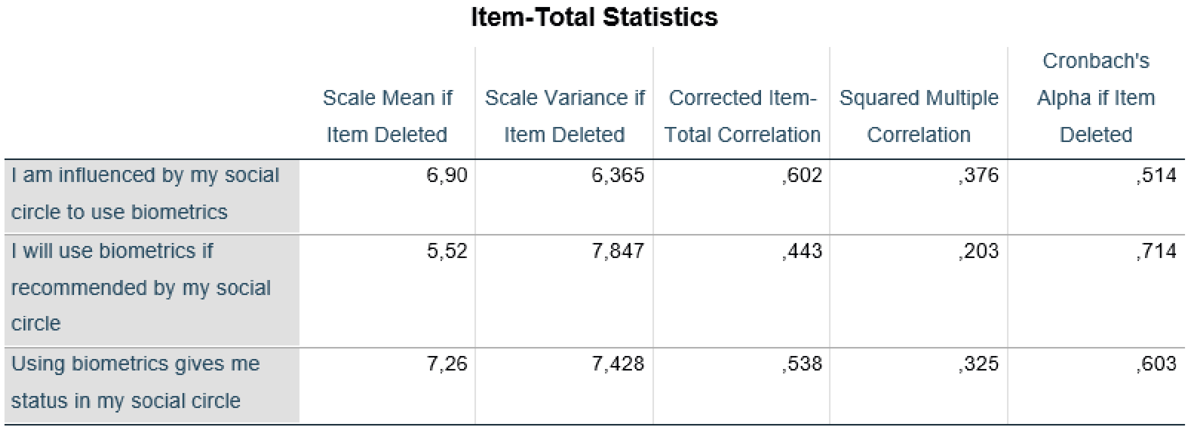
Appendix K – reliability analysis for SI without item 1

Inter-Item Correlation Matrix

	I am influenced by my circle to use biometrics	I will use biometrics if recommended by my circle	Using biometrics gives me status in my circle
I am influenced by my social circle to use biometrics	1,000	,432	,558
I will use biometrics if recommended by my social circle	,432	1,000	,346
Using biometrics gives me status in my social circle	,558	,346	1,000

Reliability Statistics

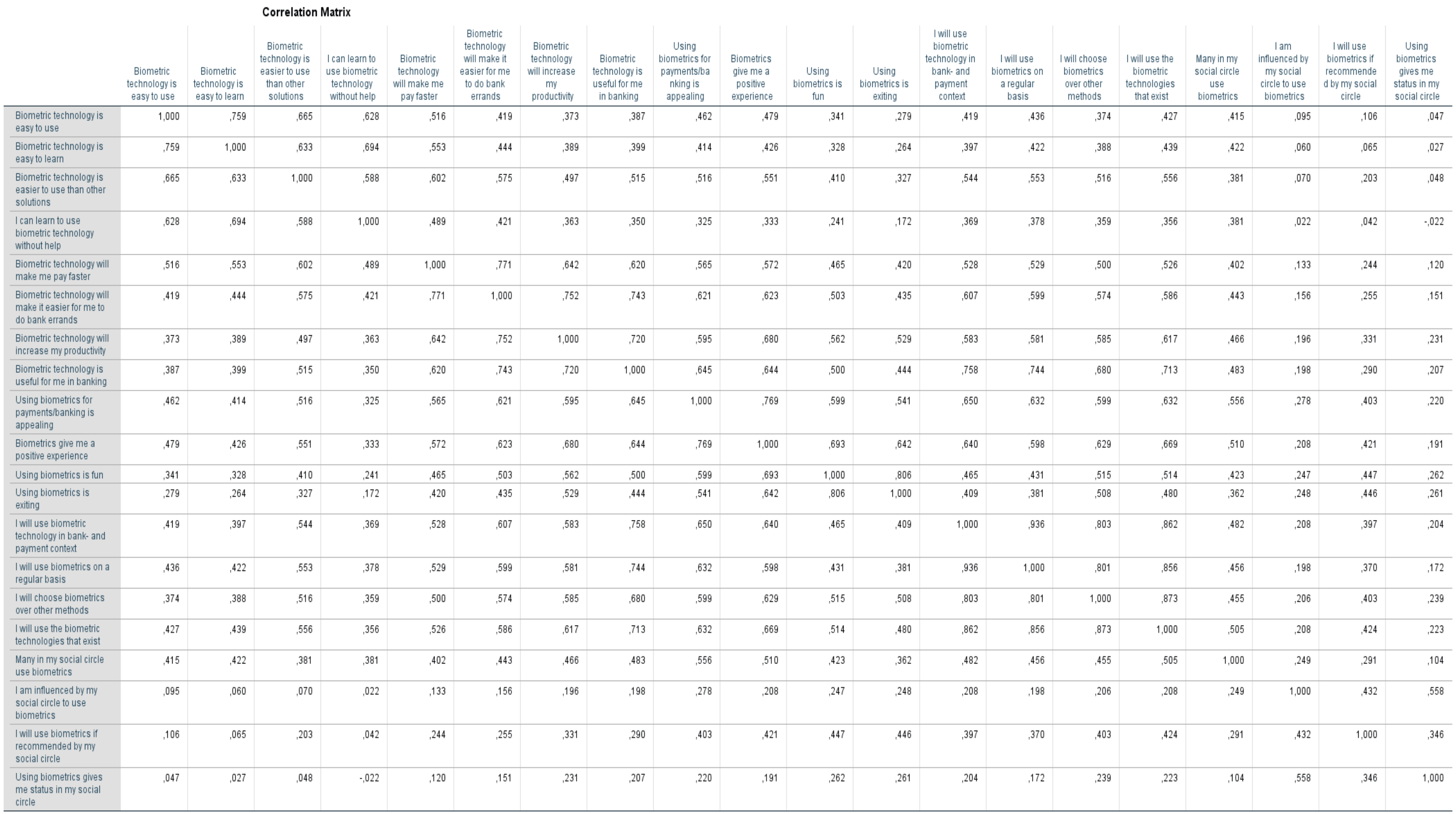
Cronbach's Alpha	Cronbach's Alpha Based on Standardized Items	N of Items
,707	,707	3



Item-Total Statistics

	Scale Mean if Item Deleted	Scale Variance if Item Deleted	Corrected Item-Total Correlation	Squared Multiple Correlation	Cronbach's Alpha if Item Deleted
I am influenced by my social circle to use biometrics	6,90	6,365	,602	,376	,514
I will use biometrics if recommended by my social circle	5,52	7,847	,443	,203	,714
Using biometrics gives me status in my social circle	7,26	7,428	,538	,325	,603

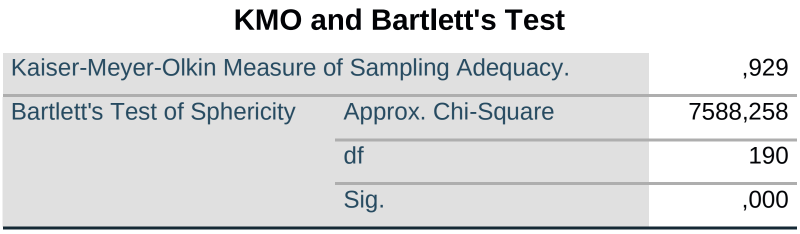
Appendix L – correlation matrix



Correlation Matrix

	Biometric technology is easy to use	Biometric technology is easy to learn	Biometric technology is easier to use than other solutions	I can learn to use biometric technology without help	Biometric technology will make me pay faster	Biometric technology will make it easier for me to do bank errands	Biometric technology will increase my productivity	Biometric technology is useful for me in banking	Using biometrics for payments/banking is appealing	Biometrics give me a positive experience	Using biometrics is fun	Using biometrics is exiting	I will use biometric technology in bank- and payment context	I will use biometrics on a regular basis	I will choose biometrics over other methods	I will use the biometric technologies that exist	Many in my social circle use biometrics	I am influenced by my social circle to use biometrics	I will use biometrics if recommended by my social circle	Using biometrics gives me status in my social circle
Biometric technology is easy to use	1,000	,759	,665	,628	,516	,419	,373	,387	,462	,479	,341	,279	,419	,436	,374	,427	,415	,095	,106	,047
Biometric technology is easy to learn	,759	1,000	,633	,694	,553	,444	,389	,399	,414	,426	,328	,264	,397	,422	,388	,439	,422	,060	,065	,027
Biometric technology is easier to use than other solutions	,665	,633	1,000	,588	,602	,575	,497	,515	,516	,551	,410	,327	,544	,553	,516	,556	,381	,070	,203	,048
I can learn to use biometric technology without help	,628	,694	,588	1,000	,489	,421	,363	,350	,325	,333	,241	,172	,369	,378	,359	,356	,381	,022	,042	-,022
Biometric technology will make me pay faster	,516	,553	,602	,489	1,000	,771	,642	,620	,565	,572	,465	,420	,528	,529	,500	,526	,402	,133	,244	,120
Biometric technology will make it easier for me to do bank errands	,419	,444	,575	,421	,771	1,000	,752	,743	,621	,623	,503	,435	,607	,599	,574	,586	,443	,156	,255	,151
Biometric technology will increase my productivity	,373	,389	,497	,363	,642	,752	1,000	,720	,595	,680	,562	,529	,583	,581	,585	,617	,466	,196	,331	,231
Biometric technology is useful for me in banking	,387	,399	,515	,350	,620	,743	,720	1,000	,645	,644	,500	,444	,758	,744	,680	,713	,483	,198	,290	,207
Using biometrics for payments/banking is appealing	,462	,414	,516	,325	,565	,621	,595	,645	1,000	,769	,599	,541	,650	,632	,599	,632	,556	,278	,403	,220
Biometrics give me a positive experience	,479	,426	,551	,333	,572	,623	,680	,644	,769	1,000	,693	,642	,640	,598	,629	,669	,510	,208	,421	,191
Using biometrics is fun	,341	,328	,410	,241	,465	,503	,562	,500	,599	,693	1,000	,806	,465	,431	,515	,514	,423	,247	,447	,262
Using biometrics is exiting	,279	,264	,327	,172	,420	,435	,529	,444	,541	,642	,806	1,000	,409	,381	,508	,480	,362	,248	,446	,261
I will use biometric technology in bank- and payment context	,419	,397	,544	,369	,528	,607	,583	,758	,650	,640	,465	,409	1,000	,936	,803	,862	,482	,208	,397	,204
I will use biometrics on a regular basis	,436	,422	,553	,378	,529	,599	,581	,744	,632	,598	,431	,381	,936	1,000	,801	,856	,456	,198	,370	,172
I will choose biometrics over other methods	,374	,388	,516	,359	,500	,574	,585	,680	,599	,629	,515	,508	,803	,801	1,000	,873	,455	,206	,403	,239
I will use the biometric technologies that exist	,427	,439	,556	,356	,526	,586	,617	,713	,632	,669	,514	,480	,862	,856	,873	1,000	,505	,208	,424	,223
Many in my social circle use biometrics	,415	,422	,381	,381	,402	,443	,466	,483	,556	,510	,423	,362	,482	,456	,455	,505	1,000	,249	,291	,104
I am influenced by my social circle to use biometrics	,095	,060	,070	,022	,133	,156	,196	,198	,278	,208	,247	,248	,208	,198	,206	,208	,249	1,000	,432	,558
I will use biometrics if recommended by my social circle	,106	,065	,203	,042	,244	,255	,331	,290	,403	,421	,447	,446	,397	,370	,403	,424	,291	,432	1,000	,346
Using biometrics gives me status in my social circle	,047	,027	,048	-,022	,120	,151	,231	,207	,220	,191	,262	,261	,204	,172	,239	,223	,104	,558	,346	1,000

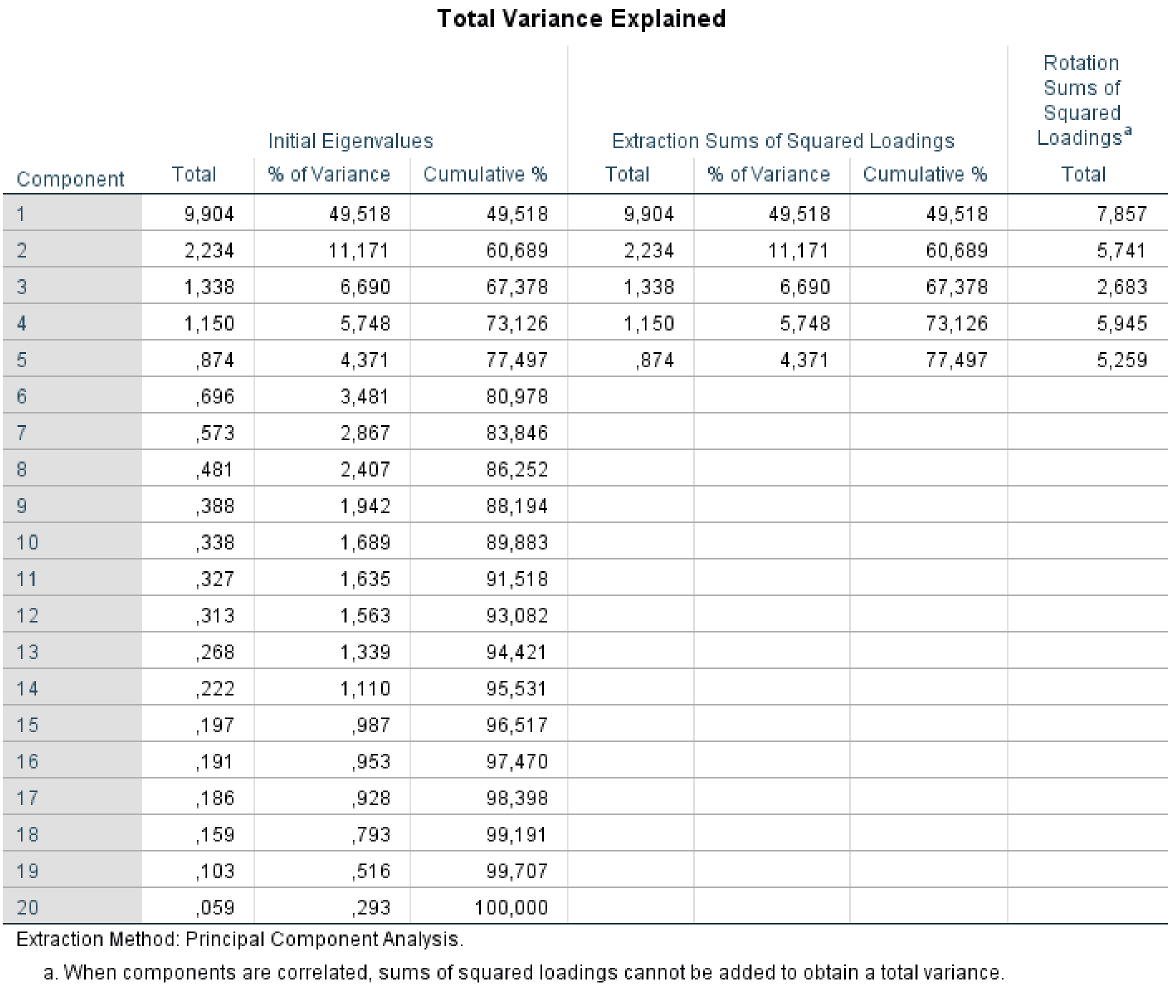
Appendix M – KMO and Bartlett’s Test



KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		,929
Bartlett's Test of Sphericity	Approx. Chi-Square	7588,258
	df	190
	Sig.	,000

Appendix N – total variance explained



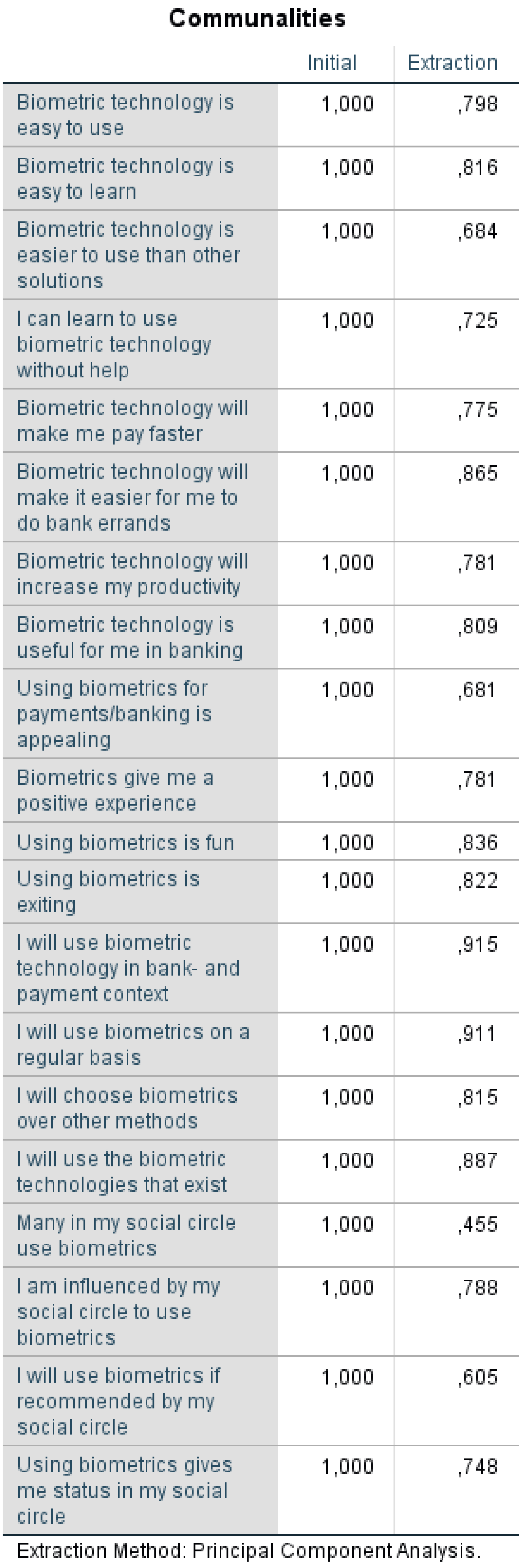
Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	9,904	49,518	49,518	9,904	49,518	49,518	7,857
2	2,234	11,171	60,689	2,234	11,171	60,689	5,741
3	1,338	6,690	67,378	1,338	6,690	67,378	2,683
4	1,150	5,748	73,126	1,150	5,748	73,126	5,945
5	,874	4,371	77,497	,874	4,371	77,497	5,259
6	,696	3,481	80,978				
7	,573	2,867	83,846				
8	,481	2,407	86,252				
9	,388	1,942	88,194				
10	,338	1,689	89,883				
11	,327	1,635	91,518				
12	,313	1,563	93,082				
13	,268	1,339	94,421				
14	,222	1,110	95,531				
15	,197	,987	96,517				
16	,191	,953	97,470				
17	,186	,928	98,398				
18	,159	,793	99,191				
19	,103	,516	99,707				
20	,059	,293	100,000				

Extraction Method: Principal Component Analysis.

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

Appendix O - Communalities

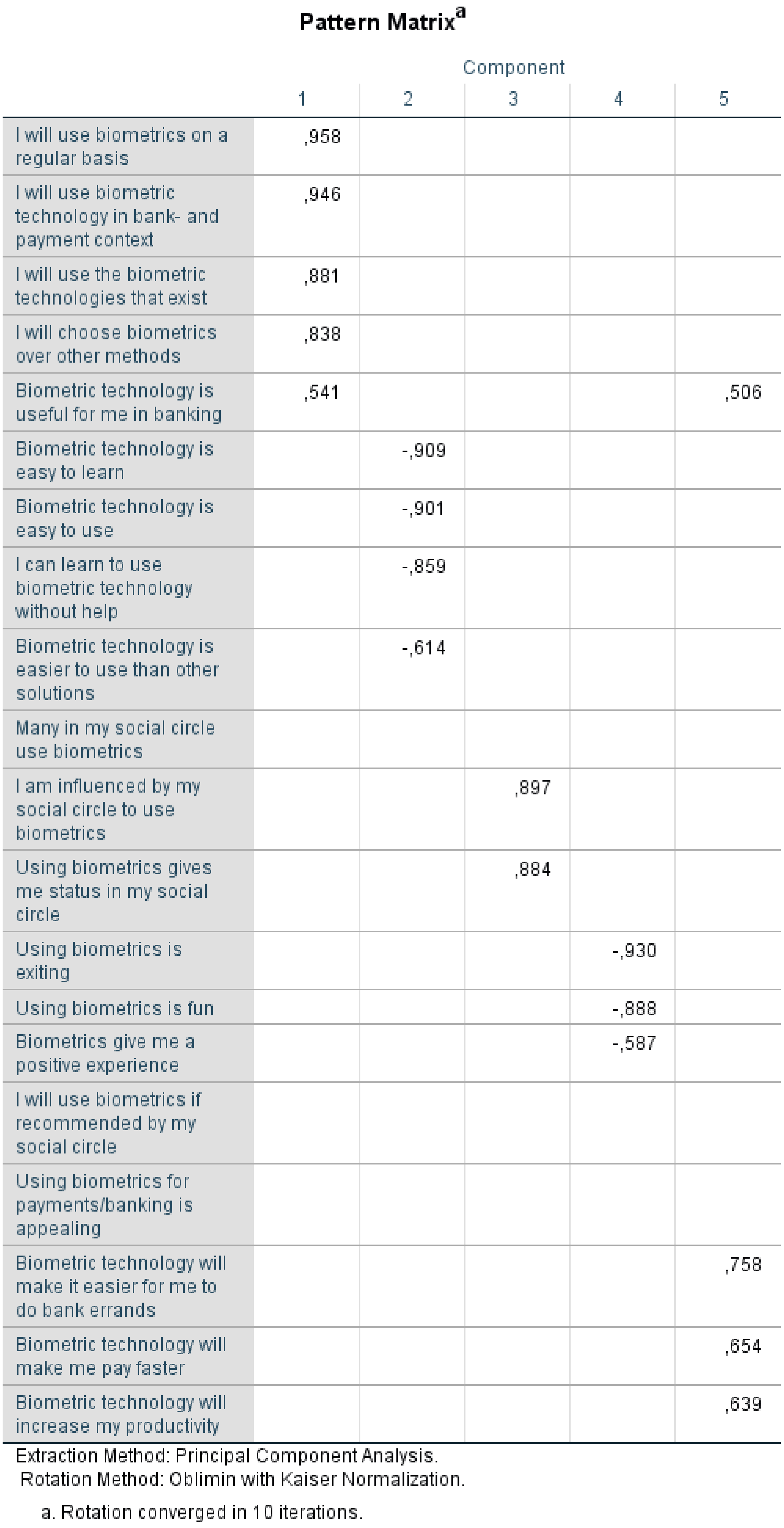


Communalities

	Initial	Extraction
Biometric technology is easy to use	1,000	,798
Biometric technology is easy to learn	1,000	,816
Biometric technology is easier to use than other solutions	1,000	,684
I can learn to use biometric technology without help	1,000	,725
Biometric technology will make me pay faster	1,000	,775
Biometric technology will make it easier for me to do bank errands	1,000	,865
Biometric technology will increase my productivity	1,000	,781
Biometric technology is useful for me in banking	1,000	,809
Using biometrics for payments/banking is appealing	1,000	,681
Biometrics give me a positive experience	1,000	,781
Using biometrics is fun	1,000	,836
Using biometrics is exiting	1,000	,822
I will use biometric technology in bank- and payment context	1,000	,915
I will use biometrics on a regular basis	1,000	,911
I will choose biometrics over other methods	1,000	,815
I will use the biometric technologies that exist	1,000	,887
Many in my social circle use biometrics	1,000	,455
I am influenced by my social circle to use biometrics	1,000	,788
I will use biometrics if recommended by my social circle	1,000	,605
Using biometrics gives me status in my social circle	1,000	,748

Extraction Method: Principal Component Analysis.

Appendix P – Pattern Matrix



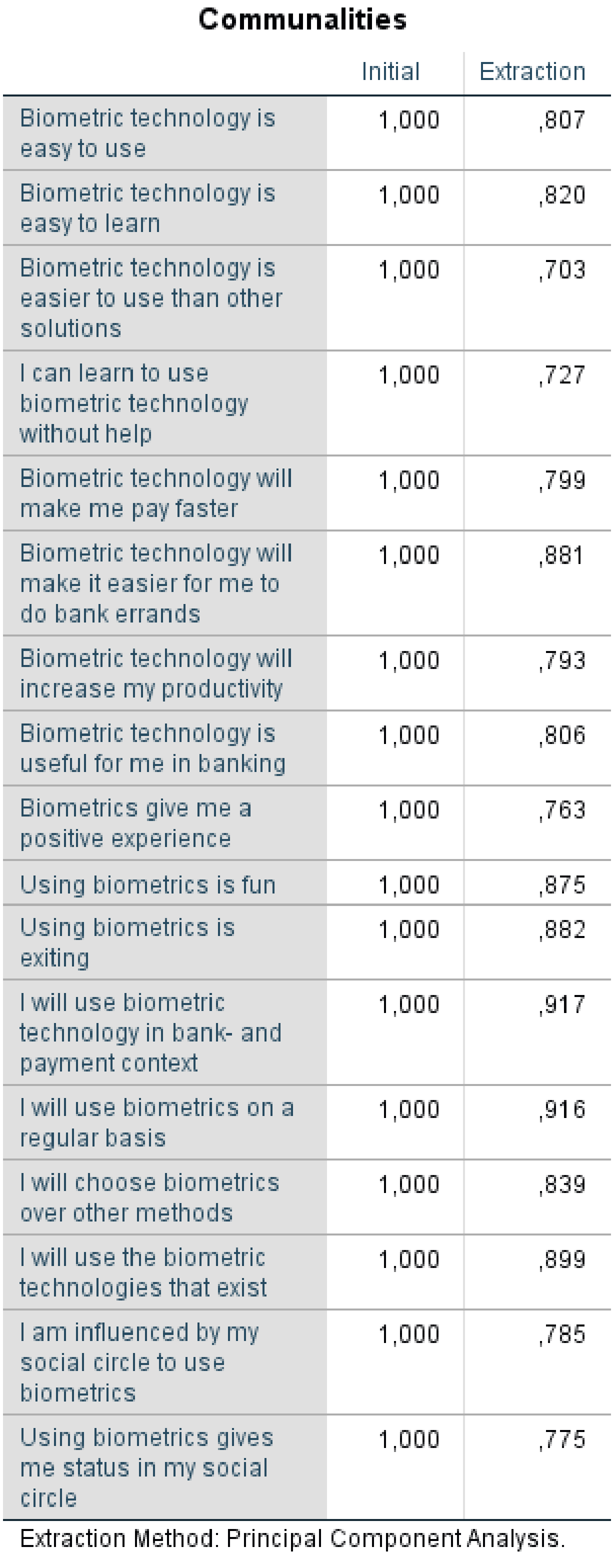
Pattern Matrix[a]

	Component				
	1	2	3	4	5
I will use biometrics on a regular basis	,958				
I will use biometric technology in bank- and payment context	,946				
I will use the biometric technologies that exist	,881				
I will choose biometrics over other methods	,838				
Biometric technology is useful for me in banking	,541				,506
Biometric technology is easy to learn		-,909			
Biometric technology is easy to use		-,901			
I can learn to use biometric technology without help		-,859			
Biometric technology is easier to use than other solutions		-,614			
Many in my social circle use biometrics					
I am influenced by my social circle to use biometrics			,897		
Using biometrics gives me status in my social circle			,884		
Using biometrics is exiting				-,930	
Using biometrics is fun				-,888	
Biometrics give me a positive experience				-,587	
I will use biometrics if recommended by my social circle					
Using biometrics for payments/banking is appealing					
Biometric technology will make it easier for me to do bank errands					,758
Biometric technology will make me pay faster					,654
Biometric technology will increase my productivity					,639

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 10 iterations.

Appendix Q – factor analysis two, communalities

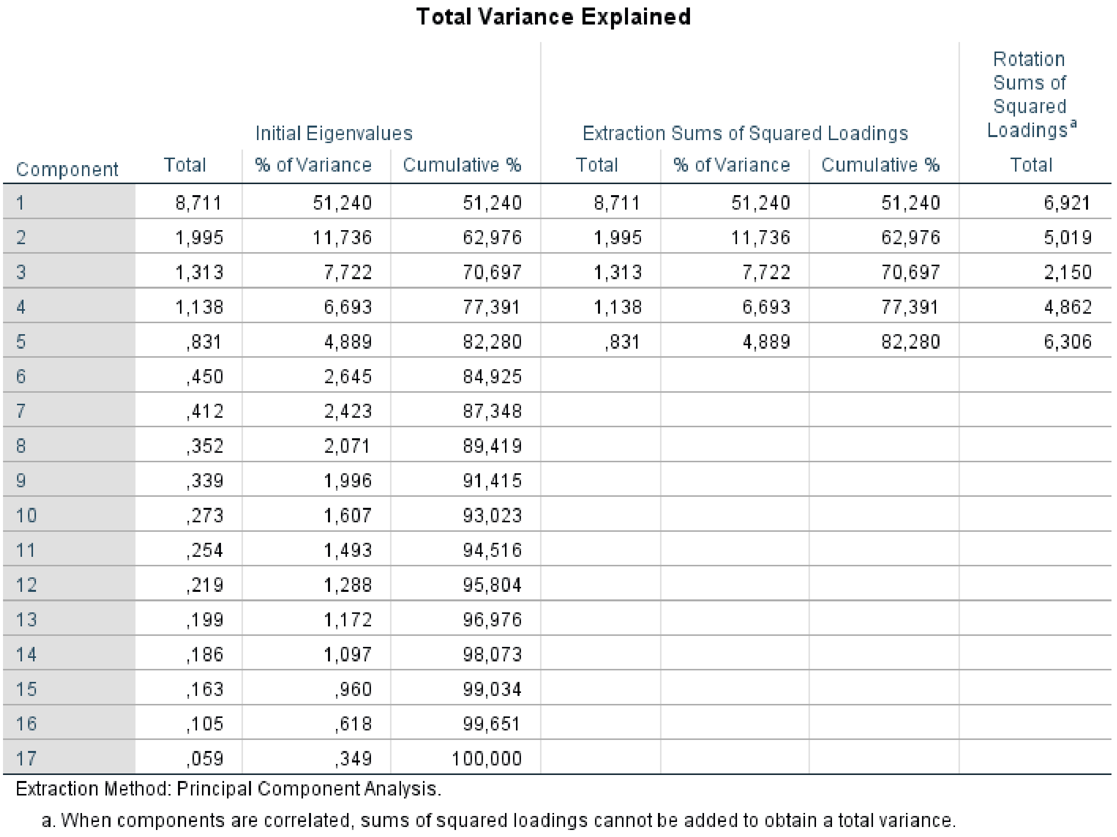


Communalities

	Initial	Extraction
Biometric technology is easy to use	1,000	,807
Biometric technology is easy to learn	1,000	,820
Biometric technology is easier to use than other solutions	1,000	,703
I can learn to use biometric technology without help	1,000	,727
Biometric technology will make me pay faster	1,000	,799
Biometric technology will make it easier for me to do bank errands	1,000	,881
Biometric technology will increase my productivity	1,000	,793
Biometric technology is useful for me in banking	1,000	,806
Biometrics give me a positive experience	1,000	,763
Using biometrics is fun	1,000	,875
Using biometrics is exiting	1,000	,882
I will use biometric technology in bank- and payment context	1,000	,917
I will use biometrics on a regular basis	1,000	,916
I will choose biometrics over other methods	1,000	,839
I will use the biometric technologies that exist	1,000	,899
I am influenced by my social circle to use biometrics	1,000	,785
Using biometrics gives me status in my social circle	1,000	,775

Extraction Method: Principal Component Analysis.

Appendix R – factor analysis two, total variance explained



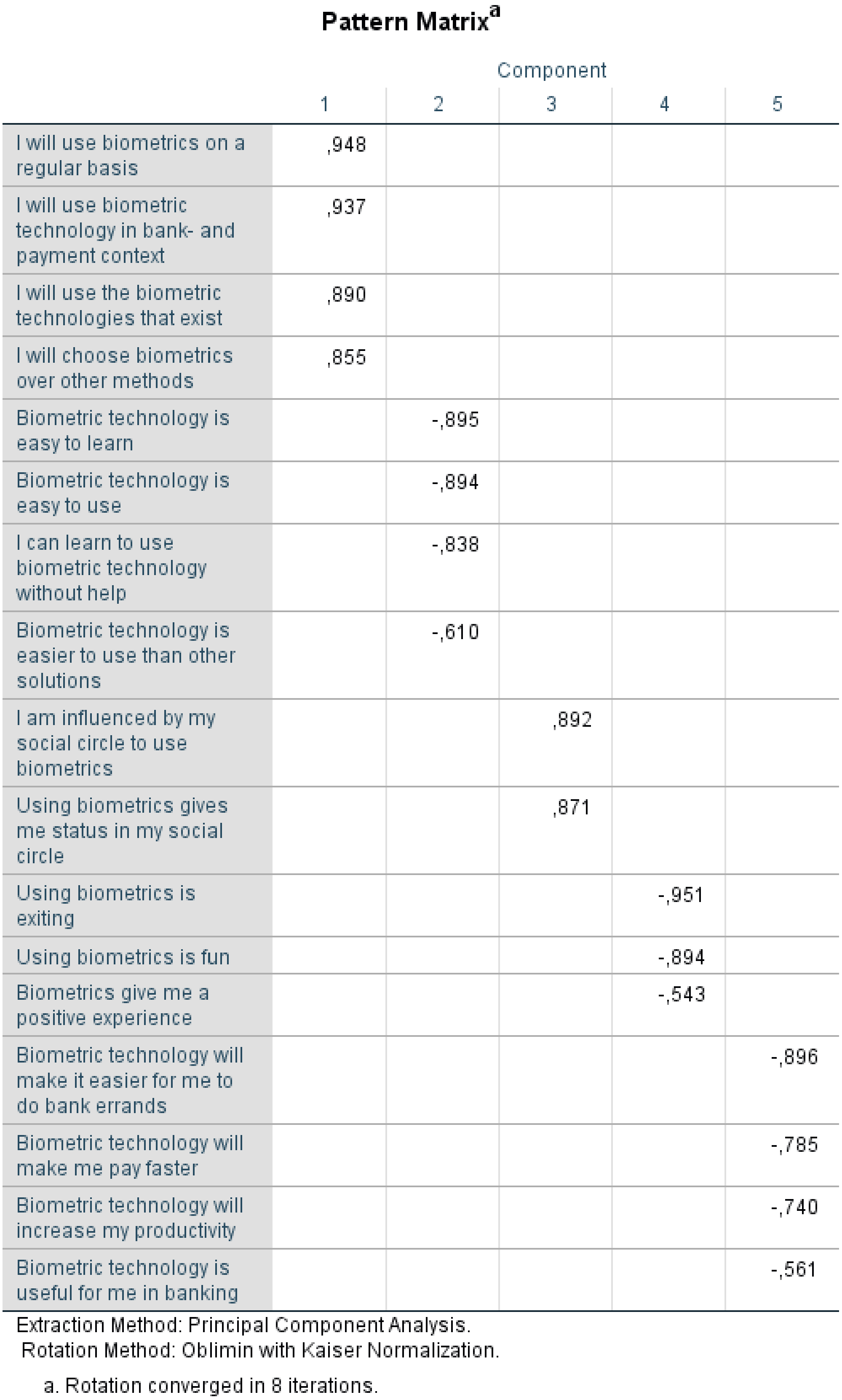
Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	8,711	51,240	51,240	8,711	51,240	51,240	6,921
2	1,995	11,736	62,976	1,995	11,736	62,976	5,019
3	1,313	7,722	70,697	1,313	7,722	70,697	2,150
4	1,138	6,693	77,391	1,138	6,693	77,391	4,862
5	,831	4,889	82,280	,831	4,889	82,280	6,306
6	,450	2,645	84,925				
7	,412	2,423	87,348				
8	,352	2,071	89,419				
9	,339	1,996	91,415				
10	,273	1,607	93,023				
11	,254	1,493	94,516				
12	,219	1,288	95,804				
13	,199	1,172	96,976				
14	,186	1,097	98,073				
15	,163	,960	99,034				
16	,105	,618	99,651				
17	,059	,349	100,000				

Extraction Method: Principal Component Analysis.

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

Appendix S – factor analysis two, Pattern Matrix



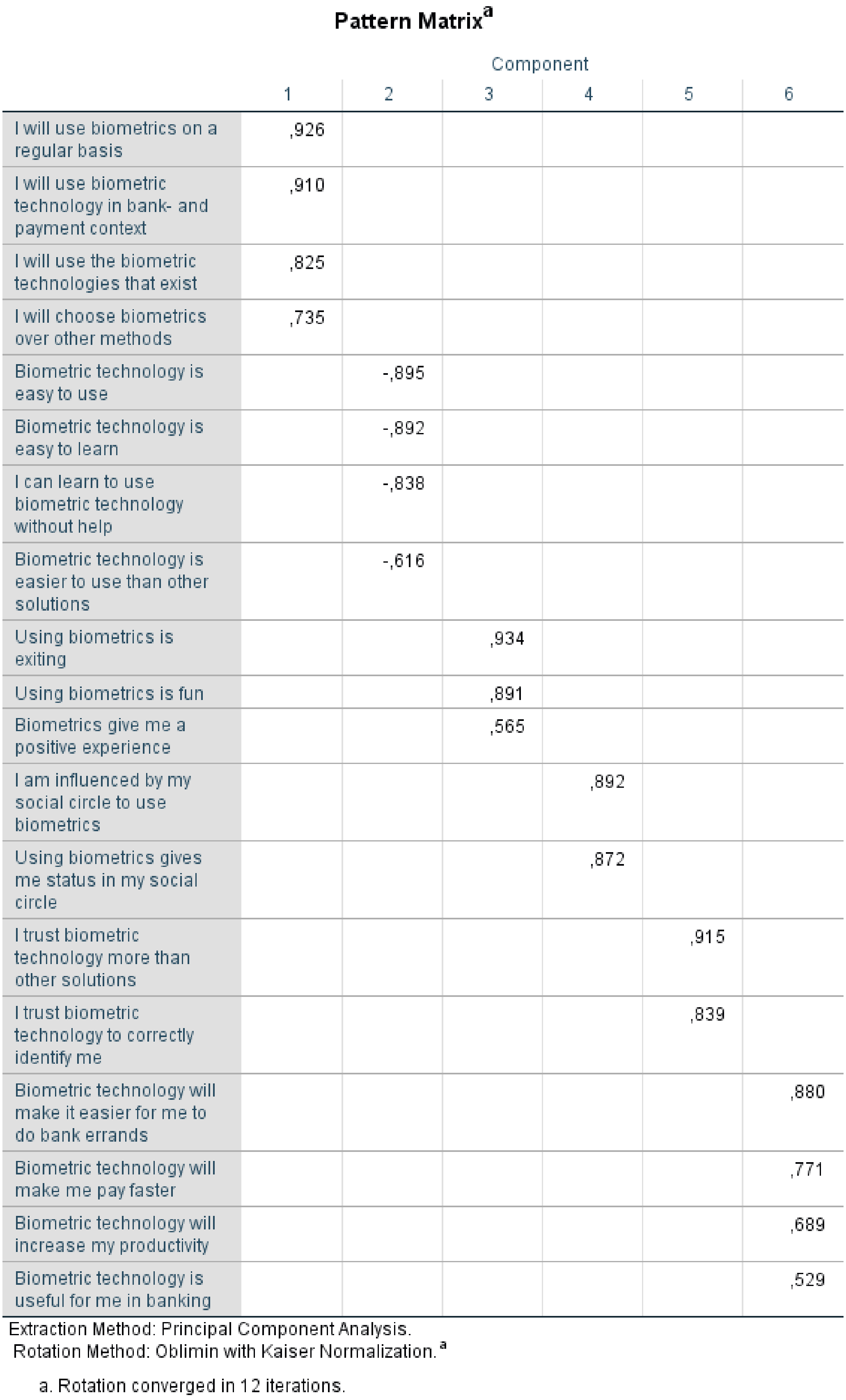
Pattern Matrix[a]

	Component				
	1	2	3	4	5
I will use biometrics on a regular basis	,948				
I will use biometric technology in bank- and payment context	,937				
I will use the biometric technologies that exist	,890				
I will choose biometrics over other methods	,855				
Biometric technology is easy to learn		-,895			
Biometric technology is easy to use		-,894			
I can learn to use biometric technology without help		-,838			
Biometric technology is easier to use than other solutions		-,610			
I am influenced by my social circle to use biometrics			,892		
Using biometrics gives me status in my social circle			,871		
Using biometrics is exiting				-,951	
Using biometrics is fun				-,894	
Biometrics give me a positive experience				-,543	
Biometric technology will make it easier for me to do bank errands					-,896
Biometric technology will make me pay faster					-,785
Biometric technology will increase my productivity					-,740
Biometric technology is useful for me in banking					-,561

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 8 iterations.

Appendix T – factor analysis three, Pattern Matrix



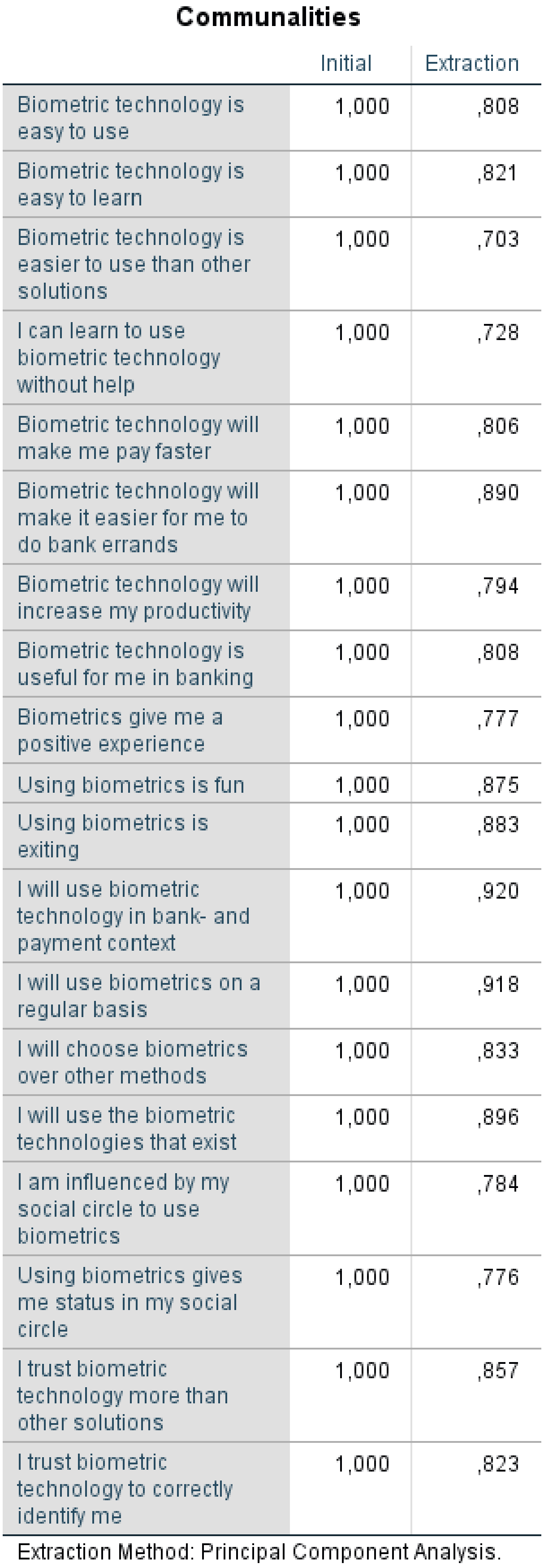
Pattern Matrix[a]

	Component					
	1	2	3	4	5	6
I will use biometrics on a regular basis	,926					
I will use biometric technology in bank- and payment context	,910					
I will use the biometric technologies that exist	,825					
I will choose biometrics over other methods	,735					
Biometric technology is easy to use		-,895				
Biometric technology is easy to learn		-,892				
I can learn to use biometric technology without help		-,838				
Biometric technology is easier to use than other solutions		-,616				
Using biometrics is exiting			,934			
Using biometrics is fun			,891			
Biometrics give me a positive experience			,565			
I am influenced by my social circle to use biometrics				,892		
Using biometrics gives me status in my social circle				,872		
I trust biometric technology more than other solutions					,915	
I trust biometric technology to correctly identify me					,839	
Biometric technology will make it easier for me to do bank errands						,880
Biometric technology will make me pay faster						,771
Biometric technology will increase my productivity						,689
Biometric technology is useful for me in banking						,529

Extraction Method: Principal Component Analysis.
Rotation Method: Oblimin with Kaiser Normalization.[a]

a. Rotation converged in 12 iterations.

Appendix U – factor analysis three, Communalities



Communalities

	Initial	Extraction
Biometric technology is easy to use	1,000	,808
Biometric technology is easy to learn	1,000	,821
Biometric technology is easier to use than other solutions	1,000	,703
I can learn to use biometric technology without help	1,000	,728
Biometric technology will make me pay faster	1,000	,806
Biometric technology will make it easier for me to do bank errands	1,000	,890
Biometric technology will increase my productivity	1,000	,794
Biometric technology is useful for me in banking	1,000	,808
Biometrics give me a positive experience	1,000	,777
Using biometrics is fun	1,000	,875
Using biometrics is exiting	1,000	,883
I will use biometric technology in bank- and payment context	1,000	,920
I will use biometrics on a regular basis	1,000	,918
I will choose biometrics over other methods	1,000	,833
I will use the biometric technologies that exist	1,000	,896
I am influenced by my social circle to use biometrics	1,000	,784
Using biometrics gives me status in my social circle	1,000	,776
I trust biometric technology more than other solutions	1,000	,857
I trust biometric technology to correctly identify me	1,000	,823

Extraction Method: Principal Component Analysis.