VILNIUS UNIVERSITY
BUSINESS SCHOOL

Management and Business Administration, Digital Marketing

OUALID AMELLAL

Susirūpinimo duomenų privatumu įtaka pasitikėjimui ir ketinimui naudotis dirbtinio intelekto pokalbių robotais internetinės bankininkystės platformose tūkstantmečio kartos atstovų tarpe	**The Influence of Data Privacy Concerns on Trust and Intention to Use AI Chatbots in Online Banking Platforms Among Millennials**

Supervisor: Dr Evelina Blažinauskytė

Vilnius, 2026

SUMMARY

VILNIUS UNIVERSITY BUSINESS SCHOOL
DIGITAL MARKETING STUDY PROGRAMME
OUALID AMELLAL

The Influence of Data Privacy Concerns on Trust and Intention to Use AI Chatbots in Online Banking Platforms Among Millennials

Supervisor – Dr Evelina Blažinauskytė
Master's thesis was prepared in Vilnius, in 2026
Scope of Master's thesis – 104 pages.
Number of tables used in the FMTP – 20 pcs.
Number of figures used in the FMTP – 4 pcs.
Number of bibliography and references – 51 pcs.

The master's thesis examines how the data privacy concerns influence the trust and intention to use AI chatbots in online banking platforms among millennials. The growing use of AI-based chatbots in online financial services is also associated with significant concerns regarding privacy, trust, and perceived risk, which directly influence the adoption by the user. The research is founded on a combined theoretical basis of the Technology Acceptance Model (TAM), Trust Theory and Privacy Calculus Theory with the aim of describing the behavioral intentions of millennial users towards AI chatbots in online banking.

Millennials have uneven adoption patterns, even though the use of AI chatbots in online banking sites is evolving at a very high rate. Such inconsistency is greatly motivated by concerns surrounding data privacy, the confidence in AI systems, and some perceived risk regarding the release of sensitive financial information. This study will be aimed at investigating how the data privacy concerns affects the trustworthiness and intention of millennials to use AI chatbots in online banking. To establish this aim, the paper evaluates data privacy concerns in AI chatbot application, synthesises the theoretical models in question, addresses the mediating influence of

trust and assesses the moderating impacts, and empirically explores the issue of millennial online banking users.

The study uses a quantitative methodological approach. The structured online questionnaire was used to minimize data collection to millennial users of internet banking services. To test the proposed research model and hypotheses, the collected data were processed with the help of descriptive statistics, analysis on reliability, correlation analysis, multiple regression analysis, mediation and moderation analysis.

The empirical analysis results suggest that the data privacy concerns has a statistically significant negative impact on the trust towards AI chatbots. The level of trust was established to be positively and significantly impacting the intention to use AI chatbots in online banking. Also, the perceptions of usefulness and the perceptions of ease of use have a positive influence on trust and intention to use. The results also indicate that the perceived risk undermines the positive domain of trust and intention to use. Also, the relationship between the concerns of privacy and trust is mediated by human-likeness and prior experience that diminish the importance of privacy-related concerns when human-likeness and prior experience are taken into consideration.

The research finds that the data privacy concerns has a central role in the connection between AI chatbots intention to use and the trust in the use of online banking. Even though millennials are aware of the efficiency and convenience of using AI chatbots, the data privacy concerns and security are used as a decisive factor in the adoption decision. Thus, online banks must prioritize data-handling transparency and high-level security, as well as a conveniently designed chatbot, to be able to inspire more users to employ AI chatbots in online customer support.

The findings of this master thesis can be reformatted into publication in academic journals specializing in the area of digital banking, financial technology or information systems research.

SANTRAUKA

VILNIAUS UNIVERSITETO VERSLO MOKYKLA
DIGITAL MARKETING STUDIJŲ PROGRAMA
OUALID AMELLAL

Susirūpinimo duomenų privatumu įtaka pasitikėjimui ir ketinimui naudotis dirbtinio intelekto pokalbių robotais internetinės bankininkystės platformose tūkstantmečio kartos atstovų tarpe

Darbo vadovė – Dr. Evelina Blažinauskytė
Magistro darbas parengtas Vilniuje, 2026 m.
Magistro darbo apimtis – 104 psl.
FMTP panaudotų lentelių skaičius – 20 vnt.
FMTP panaudotų paveikslų skaičius – 4 vnt.
Bibliografijos ir šaltinių skaičius – 51 vnt.

Magistro darbe nagrinėjama, kaip duomenų privatumo problemos veikia pasitikėjimą ir ketinimą naudotis dirbtinio intelekto (DI) pokalbių robotais internetinės bankininkystės platformose tarp tūkstantmečio kartos atstovų. Augantis DI pagrįstų pokalbių robotų naudojimas internetinėse finansinėse paslaugose taip pat siejamas su reikšmingais privatumo, pasitikėjimo ir suvokiamos rizikos klausimais, kurie tiesiogiai veikia vartotojų sprendimą juos naudoti. Tyrimas grindžiamas jungtine teorine baze, apimančia Technologijų priėmimo modelį (TAM), Pasitikėjimo teoriją ir Privatumo skaičiavimo teoriją, siekiant aprašyti tūkstantmečio kartos vartotojų elgsenos ketinimus naudotis DI pokalbių robotais internetinėje bankininkystėje.

Nors DI pokalbių robotų naudojimas internetinės bankininkystės svetainėse sparčiai auga, tūkstantmečio kartos atstovų jų naudojimo modeliai išlieka nevienodi. Šį nenuoseklumą didžiąja dalimi lemia susirūpinimas duomenų privatumu, pasitikėjimas DI sistemomis ir suvokiama rizika, susijusi su jautrios finansinės informacijos atskleidimu. Šio tyrimo tikslas – ištirti, kaip duomenų privatumo problemos veikia tūkstantmečio kartos pasitikėjimą ir ketinimą naudotis DI pokalbių robotais internetinėje bankininkystėje. Siekiant šio tikslo, darbe vertinami

duomenų privatumo klausimai DI pokalbių robotų taikymo kontekste, sintezuojami atitinkami teoriniai modeliai, nagrinėjamas tarpininkaujantis pasitikėjimo vaidmuo, vertinami moderuojantys veiksniai ir empiriškai analizuojama tūkstantmečio kartos internetinės bankininkystės vartotojų elgsena.

Tyrime taikomas kiekybinis metodologinis požiūris. Duomenims rinkti buvo naudojama struktūruota internetinė anketa, skirta tūkstantmečio kartos internetinės bankininkystės paslaugų naudotojams. Siūlomam tyrimo modeliui ir hipotezėms patikrinti surinkti duomenys buvo analizuojami taikant aprašomąją statistiką, patikimumo analizę, koreliacinę analizę, daugialypę regresinę analizę, mediacijos ir moderacijos analizę.

Empirinės analizės rezultatai rodo, kad duomenų privatumo problemos turi statistiškai reikšmingą neigiamą poveikį pasitikėjimui DI pokalbių robotais. Nustatyta, kad pasitikėjimo lygis teigiamai ir reikšmingai veikia ketinimą naudotis DI pokalbių robotais internetinėje bankininkystėje. Taip pat suvokiamas naudingumas ir suvokiamas naudojimo paprastumas daro teigiamą įtaką tiek pasitikėjimui, tiek ketinimui naudotis. Rezultatai taip pat rodo, kad suvokiama rizika silpnina teigiamą pasitikėjimo ir ketinimo naudotis poveikį. Be to, ryšys tarp privatumo problemų ir pasitikėjimo yra tarpininkaujamas žmogiškumo (human-likeness) ir ankstesnės patirties, kurie sumažina privatumo problemų svarbą, kai šie veiksniai yra įtraukiami į analizę.

Tyrimas atskleidžia, kad duomenų privatumo problemos atlieka esminį vaidmenį ryšyje tarp ketinimo naudotis DI pokalbių robotais ir pasitikėjimo internetinės bankininkystės kontekste. Nors tūkstantmečio kartos atstovai suvokia DI pokalbių robotų naudojimo efektyvumą ir patogumą, duomenų privatumas ir saugumas išlieka lemiamais veiksniais priimant sprendimą dėl jų naudojimo. Todėl internetiniai bankai turėtų teikti pirmenybę duomenų tvarkymo skaidrumui, aukšto lygio saugumui bei patogiam ir gerai suprojektuotam pokalbių robotui, siekdami paskatinti didesnį vartotojų įsitraukimą į DI pagrįstą klientų aptarnavimą.

Šio magistro darbo rezultatai gali būti pritaikyti publikacijoms akademiniuose žurnaluose, besispecializuojančiuose skaitmeninės bankininkystės, finansinių technologijų ar informacinių sistemų tyrimų srityse.

LIST OF ABBREVIATIONS

General & Theoretical Abbreviations

AI : Artificial Intelligence

TAM : Technology Acceptance Model

UTAUT : Unified Theory of Acceptance and Use of Technology

NLP : Natural Language Processing

ECT : Expectation-Confirmation Theory

Gen Z : Generation Z

Study Variable Abbreviations

DPC : Data Privacy Concerns

TR : Trust in AI Chatbots

PU : Perceived Usefulness

PEOU : Perceived Ease of Use

PR: Perceived Risk

HL : Human-Likeness

PE : Prior Experience

IU : Intention to Use AI Chatbots

Table of Contents

INTRODUCTION

Artificial intelligence (AI) is now a pillar of innovation, efficiency, and customer interaction in the fast-paced digital financial services sector. The AI-powered chatbots is one of the most groundbreaking and disruptive uses of AI in this industry, a chat agent that is capable of simulating and imitating human language and interaction and helps customers with the daily tasks, i.e., account inquiries and processing transactions and personalized financial advice. Some of the technologies, including natural language processing (NLP) and machine learning, are employed to interpret the queries of the user and respond in rea time, provided by chatbots (Coopamootoo and Toreini, 2020; Cheng and Jiang, 2020).

Institutions such as banks and fintech firms are strongly implementing chatbots into their online and mobile platforms to improve customer experience, enhance service availability and reduce the costs. According to Kelly et al. (2022), the use of chatbots has increased quickly among al thee customer interacting industries, with banking being one of the most proactive in implementing the technology. These chatbots offer 24/7 service, handle repetitive inquiries, and serve as a link between digital platforms and human service agents, even often replacing the traditional customer service channels.

Across the user demographic categories most effected by the shift are millennials (born between 1981 and 1996), as digital natives, millennials are skilled at using technology and represent one of the most prominent groups of online banking users. Their preferences include real-time communication, seamless app functionality, and autonomy in financial decision-making (Uddin et al., 2024; Suhartanto et al., 2022). This places them as a critical target audience for the banks introducing conversational AI into their service offerings. Nonetheless, despite the technologic literacy that millennials are famously endowed with their awareness of data privacy and ethical usage of technology can be described as a peculiar feature of this generation. With growing fears that personal and financial information in prone to being hacked, that algorithmic favoritism and sharing takes place, millennials tend to weigh convenience against caution. Past data indicate that the of data privacy concerns in relations to the way personal information is gathered, stored, and utilized may have a significant effect on the trust of the users in AI systems (AI chatbots) Giordani, 2023; Lappeman et al., 2022). This tension between the appeal of technological convenience and the anxiety surrounding data misuse underpins the complex relationship millennials have with AI chatbots in banking.

Although nowadays there are a lot of chatbots in banking, the actual usage among millennials is inconsistent. While some users embrace the technology for its speed and efficiency, others stay hesitant due to the issue of the transparency, accountability, and the ability to protect

personal data. Research has shown that the perceived risk that comes with chatbots interactions, especially those involving in financial data usually leads with resistance or conditional use (Hasan et al., 2023; Shaikh et al., 2023).

Numerous studies have applied frameworks such as the Technology Acceptance Model (TAM) or the Unified Theory of Acceptance and Use of Technology (UTAUT) to test chatbot adoption. These models examen the usefulness and ease of use but often underrepresent psychological and ethical variables such as trust and privacy (Patil & Kulkarni, 2019; Cheng & Jiang, 2020). Additionally, while trust has been recognized as a critical factor in human-computer interaction, literature lacks empirical depth in understanding how trust mediates the relationship between privacy concerns and behavioral intention, often it seen within the financial sector and among millennials. Furthermore, although some research has explored used experience with AI in banking (Bhattacharya & Sinha, 2022; Lubbe et al., 2025; Toh & Tay, 2022), few studies have conducted targeted investigations into how data privacy concerns specifically shape trust (Lappeman et al., 2022; Giordani, 2023; Luo et al., 2021), and how that trust influences the intention to use chatbots. The role of individual differences, such as prior experience with chatbots or perceptions of human-likeness, also remains underexplored in this context Thanh & Linh, 2024; Ngu Ngendi, 2024). Therefore, this lead to the central problem of this research:

How Data Privacy Concerns Influence Trust and Intention to Use AI Chatbots in Online Banking Platforms in the Case of Millennials?

By addressing this question, this study aims to investigate the data privacy influence on millennials' trust and intention to use AI chatbots within online banking platforms.

The study objectives are as follows to accomplish this goal:

1. To analyze the concept of data privacy concerns and examine their relevance in the context of AI chatbot use within online banking platforms.
2. To identify and critically compare the main theoretical models and empirical findings related to data privacy, trust, technology acceptance, and behavioral intention in digital financial services.
3. To examine the role of trust as a mediating mechanism and the roles of perceived risk, human-likeness, and prior experience as moderating factors in the relationship between data privacy concerns and millennials' intention to use AI chatbots in online banking.
4. To develop a research methodology and conduct an empirical study among millennial online banking users in order to determine which factors significantly influence trust and intention to use AI chatbots.

5. To interpret the empirical findings in light of existing literature and, based on these results, formulate integrated theoretical conclusions and practical recommendations for banks, chatbot developers, and future researchers aimed at enhancing trust, transparency, and the secure adoption of AI chatbots in online banking.

This study thus builds a multi-layered conceptual mode, grounded in Privacy Calculus Theory, Trust Theory, and the Technology Acceptance Model, to provide a comprehensive understanding of millennial user behavior.

The master thesis spit into six chapters with each chapter built on the knowledge of the previous one, in order to examine the research problem in a systematic manner.

- **Chapter 1** is a literature review of the pertinent literature. It addresses the development of AI chatbots in online banking and its functionality, the digital behavior and privacy attitudes of millennials, and the theoretical framework of the research, such as the Technology Acceptance Model (TAM), the Trust Theory and the Privacy Calculus Theory. In accordance with this review, the main constructs and conceptual structure of the research are elaborated.
- **Chapter 2** outlines the research methodology that was used in the study. It describes research design, population and sampling approach, data collection tool, measurement scales, and other ethical considerations. The analysis methods used in quantitative data analysis are also described in the chapter such as descriptive statistics, reliability analysis, correlation analysis, multiple regression, mediation and moderation analysis.
- **Chapter 3** discusses and provides the outcomes of the empirical study. This chapter contains a demographic profile of the respondents, the descriptive statistics, reliability, and validity test of the measurement tools, and the hypothesis test results. Then they critically discuss the empirical findings against the previous works and identify the contributions to theory and the managerial implications.
- **Chapter 4** is the final chapter it concludes the thesis with a summary of the key empirical results, academic and practical implications of AI chatbots on the online banking industry on the developers of AI chatbots, and a set of recommendations to enhance trust, transparency, and safe adoption of AI chatbots in online banking. The chapter discusses also the limitations of the study and presents the directions of the further research.

1. THEOREETICAL ANALYSIS OF TRUST AND DATA PRIVACY CONCERNS IN THE USE OF AI CHATBOTS IN ONLINEE BANKING

1.1 AI chatbots in online banking and their definition, evolution and functional role

Artificial intelligence (AI) has transformed the relationship between banks and customers through the integration of artificial intelligence in digital financial services. The most notable advances in this field have been AI-powered chatbots automated, conversational, agents that mimic human-like conversation via a text interface or voice interface. In a broad definition, a chatbot refers to a software program that is employed to have an on-line chat dialogue either through text or text-to-speech, instead or offering direct contact with a living human agent (Wube et al., 2022). These are systems that are based on natural language processing (NLP), machine learning, and sentiment analysis to understand user queries, learn through past interactions, and become better at responding to them over time (Bhattacharya & Sinha, 2022).

Chatbots have reached a high level of intelligence and context-sensitive agents, compared to the rule-based scripts. The initial versions were restricted to linear chain-trees of questions and answers, which could never be modified to accommodate process questions. Having evolved into both NLP-based and deep learning models, current chatbots provide users with real-time and customized services, and are often embedded right into banking websites, applications, and messaging systems (Satheesh & Nagaraj, 2021). They are also used in banking to assist a broad set of tasks such as balance inquiries, transaction histories, credit score inquiries, fraud detection, and even investment advice (Toh & Tay, 2022). These functions do not only save the cost of customer service, but they also expand the access to the financial services.

Chatbots are more likely to gain popularity in the field of online banking due to the transition to customer-oriented digital transformation. Chatbots have also been embraced by banks as users seek greater immediate response, personalization, and 24/7 service. Mucsková (2024) emphasizes that AI-based solutions such as chatbots can assist banks in addressing the needs of consumers in real-time, increasing the scope of their operations, and acquiring useful customer data to further improve interactions with them. Moreover, the interfaces with chatbots may seem less frightening than actual human interaction, particularly when handling a sensitive topic like account error or loan application (Kumar et al., 2025).

Efficiency and cost-effectiveness are one of the most important advantages of AI chatbots in the banking sphere. The aspect of availability and scalability is a limiting factor to traditional call

centers, which are human operated. Chatbots, on the other hand, are capable of serving many clients at once, reducing waiting time and enhancing customer satisfaction (Rahman et al., 2023). Banks such as Bank of America (with Erica) and Capital one (with Eno) have demonstrated that chatbots could dramatically decrease the volume of customer support and also boost customer engagement. Consequently, the chatbot technology has become a part of the digital strategy of financial institutions (Kelly et al., 2022; Mucsková, 2024; Rahman et al., 2023).

Nonetheless, the implementation of chatbots in online banking is not free of difficulty. The matters of security, data privacy, and trust keep influencing how people view chatbots in terms of reliability. Whereas Wube et al. (2022) focus on data privacy as the main obstacle, Bhattacharya and Sinha (2022) also say that personalization and quality of services are equally important in long-term user engagement. These opposite results imply that privacy is both a necessary but not a sufficient condition of intention to use and combined models that consider both technical and psychological predictors of trust are required. A systematic review by Wube et al. (2022) indicates that although customers enjoy the convenience of AI bots, the collection, processing, and storage of their data are of concern. Since banking information is sensitive, chatbots should be able not only to work effectively but also to comply with the data protection principles and provide an impression of digital reliability (Mucsková, 2024).

Although these are the concerns, the pace of the usage of chatbots is increasing. Kelly et al. (2022) conducted a multi-industry analysis according to which banking was among the most rapidly expanding industries in chatbot deployment and listed increasing user expectations, the pandemic-driven changes in digital shifts, and greater readiness of banks to invest in AI infrastructure. This is in line with the observation of Bhattacharya and Sinha (2022) that banking customers, particularly those who belong to younger generations, exhibit a greater level of acceptance in the case when chatbots are viewed as helpful, responsive, and secure. This puts a paradox in the literature: even though Suhartanto et al. (2022) identify convenience as a leading cause of loyalty, Pelote (2022) demonstrates that privacy concerns may prevail over convenience in case of weak institutional protection. Such divergent views imply that millennials consider trade-offs in different situations under assurances of security in context.

To summarize, AI chatbots are now an important part of contemporary web-based banking services. They offer clients low-cost, scalable and immediate service solutions and enable the banks to simplify the operations and maximize user satisfaction. Their further adoption is, however, dependent not only on functional capabilities but also on the extent to which these

systems can respond to user fears on matters of privacy, trust and human-like interaction themes which are discussed in det ails in the subsequent sections of this literature review.

1.2 Theoretical Framework and Conceptual Foundations of the Study

1.2.1 Technology Acceptance Model (TAM) and its Foundations and Relevance to AI Chatbots in Online Banking

One of the most popular theoretical models that have been applied in the field of information systems is Technology Acceptance Model (TAM), which was introduced by Davis (1989). TAM is an explanation of how users will accept and utilize a technology but emphasizes two main beliefs that include Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). Perceived Usefulness is the level of how an individual believes that the use of a specific system will make his or her performance better when Perceived Ease of Use is a degree of how the individual believes that using the system will be effort free. Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) together determine the attitude of an individual towards the use of a technology and the latter affect their behavioral intention to use which is the closest predictor to actual usage (Davis, 1989).

Below, in figure 1, the model of the Technology Acceptance Model is presented.

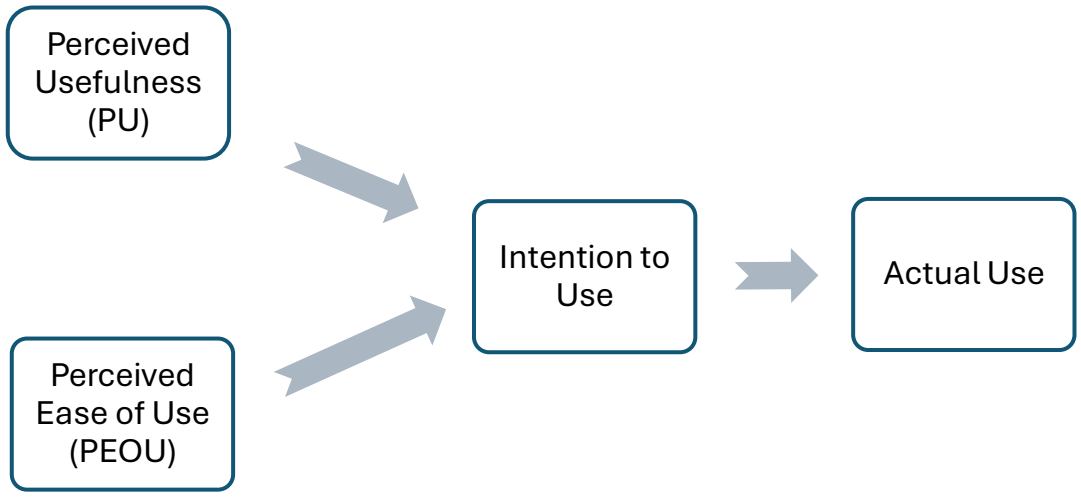


Figure 1. Extended Technology Acceptance Model incorporating Trust and Privacy Concerns in the context of AI Chatbots in Online Banking (adapted from Davis, 1989).

Technology Acceptance Model (TAM) can be applied to the online banking and AI chatbots situation to a considerable degree. The target group, or millennials, was more likely to judge digital technologies according to the capacity to present a smooth efficient and easy-to-use experience (Venkatesh and Davis, 2000; Lappeman et al., 2022). In the banking industry, Perceived Usefulness (PU) is the index that reveals the quality of the user believing that chatbots can help them fulfill their financial transactions more effectively and faster than the traditional medium, whereas Perceived Ease of Use (PEOU) is the measure that depicts the extent to which users believe that the chatbot interface is user-friendly and intuitive (Davis, 1989; Venkatesh and Bala, 2008). There have always been empirical studies that confirm the explanatory value of TAM in forecasting behavioral intention with regard to financial technologies and AI-based services (Luo et al., 2021; Giordani and Ferreira, 2023).

Thanth and Linh (2024) discovered that the Perceived Ease of Use had a significant influence on the adoption of e-banking chatbots by Gen Z customers in Vietnam. In a similar vein, Toh and Tay (2022) were able to show that the factor of perceived usefulness is a key driver in millennials adopting chatbots in Malaysian banks. Another study by Lubbe et al. (2025) also indicated that the positive experience with chatbot efficiency leads to its further use by millennials in the new markets.

In the long run, scholars have expanded TAM to include psychological and ethical aspects in consideration of the fact that simply functional considerations (usefulness and ease of use) do not suffice to explain the use of technology in situations where sensitive data are involved. Shaikh et al. (2023) combined trust and perceived risk into TAM to describe customer intention to use banking chatbots and Mehrolia et al. (2023) stated that such ethical as data privacy concerns are underrepresented in TAM research. This gap highlights the importance of the inclusion of TAM with other related frameworks like Trust Theory and Privacy Calculus Theory in order to bring in psychological and ethical aspects of the use of technology in high-stakes contexts such as online banking.

The current study thus is a structural foundation of TAM but adds constructs of trust and privacy concerns as antecedent factors influencing behavioral intention, with trust acting as a mediating variable. In this way, it acknowledges that the intention to use AI chatbots does not only rely on the perceptions of usefulness and ease of use but the degree of trust that millennials have in the technology and the capacity of the bank to secure their data.

1.2.2 Trust Theory and its Institutional and Technology Trust in Digital Financial Services

The Trust Theory is one of the frameworks that can be used to explain technology acceptability when dealing with uncertainty and sensitive information. According to Mayer, Davis and Schoorman (1995) trust is a readiness of one side to be vulnerable to the actions of the other on the basis of the belief that the other party will do a specific action that is of interest to the party doing the trusting. That is, the trust dimension occurs where a user is convinced that an organization or technology is capable, dependable and that it behaves in an honesty manner. Trust, in this case, is a key factor in digital financial services since the personal and financial information of consumers is highly sensitive, and thus consumers will only use tech-based services (AI-powered chatbots) on the condition that they trust them.
Below, in figure 2, the model of the Trust Theory is presented.

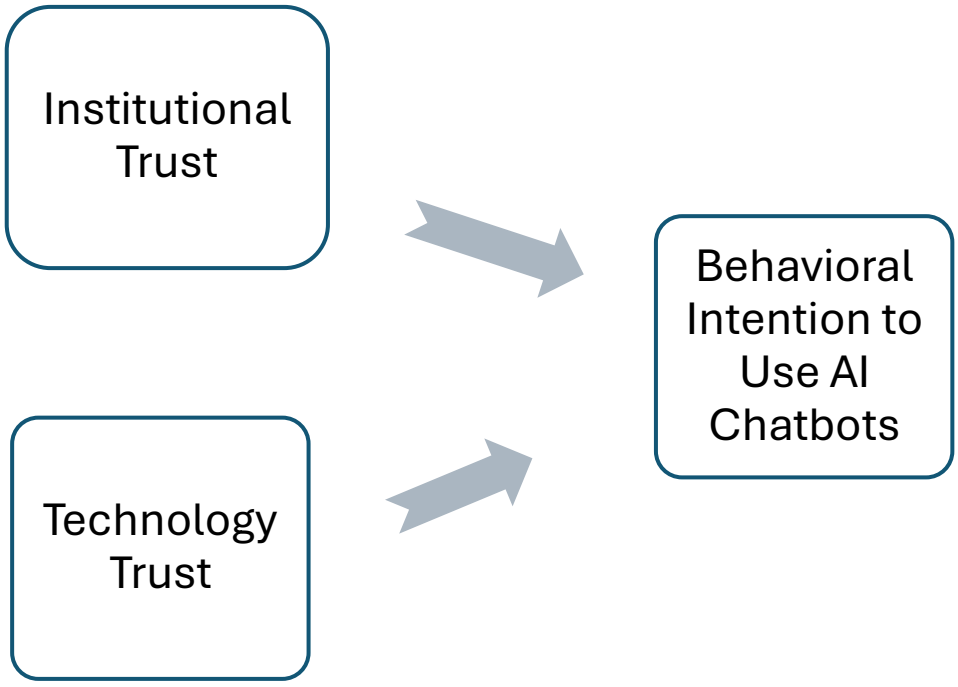


Figure 2. Trust Theory applied to AI Chatbots in Online Banking (adapted from Mayer et al., 1995).

In the case of chatbots in online banking, it is possible to define trust in two dimensions, i. e., institutional trust (the trust in the bank or other financial institution that offers the service) and technology trust (the trust in the chatbot as a technological interface) (Lappeman et al., 2022; Luo et al., 2021). The institutional trust is associated with the appraisal of the bank reputation, data protection policies, and adherence to regulations, and the technology trust is connected with the

reliability of the chatbot, its safety, and technical functionality. Users can only share sensitive financial data and perform transactions through AI-driven interfaces with both types of trust.

Studies have shown that trust is a key factor in the use and further utilization of chatbots in banking repeatedly. As Lappeman et al. (2022) demonstrated, the desire of millennials to share personal data with banking chatbots is highly contingent on their degree of trust toward the bank and the chatbot. On the same note, Luo et al. (2021) discovered that trust positively influences perception of risk and desire to use chatbots. The fact that millennials seek secure authentication, open communication, and understanding interactions to establish trust also indicates that technical and relational cues are important (Alagarsamy and Mehrolia, 2023). Rohit et al. (2025) also indicated that consumer interactions with smart banking chatbots are highly affected by the two issues of trust and privacy.

The concept of initial trust is significant to the Trust Theory, and it is the trust that a user forms before they have a long personal experience with a technology. First trust may be especially important to millennials, who tend to be innovators when it comes to digital solutions and are also concerned about cyberattacks and privacy breaches (Luo et al., 2021). Human-likeness (anthropomorphism) is a design concept in this context, as it may increase trust through making interactions more natural and socially present (Sfar et al., 2025), but over anthropomorphism can suggest the possibility of manipulation or other administrative goals (Ng et al., 2020).

The Technology Acceptance Model is therefore a complement of the Trust Theory since it is clear that psychological confidence in data security and institutional reliability is the cause of behavioral intention which cannot be solely based on a sense of usefulness or the ease with which the system can be used. Trust is represented as a mediator between the factors of data privacy concern and intention to use in this thesis, and this reflects the key role of trust in the transformation of privacy perceptions into behaviors.

1.2.3 Privacy Calculus Theory and its Balancing Benefits and Risks in Data Disclosure

The Theory of Privacy Calculus (Culnan and Armstrong, 1999) describes the way people decide whether or not to reveal personal information in digital space. This theory posits that the users do a cost-benefit analysis of the potential costs (the possible risks, which include loss of control over their personal data, data misuse, and identity theft) and the potential benefits (convenience, personalization, and efficiency). The result of this in-house calculation is what will

decide whether they will utilize a technology or service. Privacy Calculus has been used extensively regarding e-commerce, internet banking and social media, but comparatively few studies have used it directly in AI chatbot settings in the financial industry.

Below, in figure 3, the model of Theory of Privacy Calculus is presented.

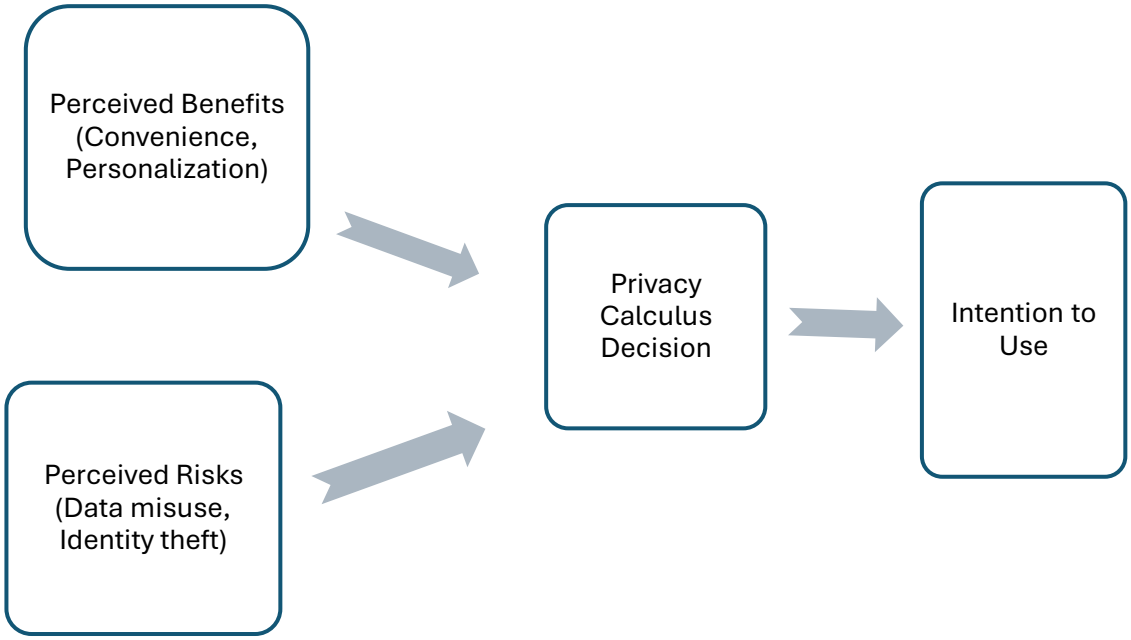


Figure 3. Privacy Calculus Theory applied to AI Chatbots in Online Banking (adapted from Culnan & Armstrong, 1999).

The Privacy Calculus Theory is particularly applicable to millennials in terms of online banking chatbots since this group of individuals is both digitally literate and privacy aware. Studies indicate that this generation considers the utility of AI chatbots (e.g., 24/7, instant response, saving time) and the risks (e.g., sharing financial information, fraud, cyberattacks) in a ratio. Bouhia et al. (2022) discovered that the issue of privacy of customers affects their desire to use chatbots in customer service interactions. On the same note, Giordani (2024) suggested that AI breaches of privacy in the banking sector are major threats to the confidence of consumers. Lappeman et al. (2022) proved that millennials are ready to provide personal data only when they are sure that institutions have powerful protection systems implemented, which supports the cost-benefit reasoning of a privacy calculus.

Trust is an important aspect of Privacy Calculus. Customers who have high trust in a bank or chatbot will feel that there are fewer risks and thus they will be more ready to share personal information or utilize the service. On the other hand, distrust increases the perceived risk and decreases the desire of involvement (Hasal et al., 2021; Luo et al., 2021).

Privacy Calculus is also a complement to TAM as it adds an additional perspective on the concept of usability, namely ethical and emotional aspects. As TAM is used to describe the impact of usefulness and ease of use as explanatory factors of intention, there is Privacy Calculus that describes the possibility of a useful, easy-to-use system being rejected in case the perceived risks of privacy are too high. This paper will combine Privacy Calculus, Trust Theory, and TAM, which will give a more comprehensive understanding of how millennials decide to use AI chatbots in online banking.

1.2.4 Theoretical Integration of TAM, Trust Theory, and Privacy Calculus

To understand the adoption and interaction of millennials with AI chatbots in online banking services, the combination of the Technology Acceptance Model (TAM), Trust Theory, and Privacy Calculus can be viewed as a complex approach to the issue. All the theories provide a unique point of view that, together, can give a more detailed explanation of the cognitive, emotional and ethical aspects affecting user behavior.

TAM (Davis, 1989) focuses on the functional and cognitive issues that contribute to the adoption of technology, and they are perceived usefulness and perceived ease of use. These constructs identify the extent of the belief that individuals have concerning the use of a technology in improving their performance and with minimal effort. In the framework of AI-driven chatbots in the context of online banking, TAM is capable of describing the way users consider the effectiveness, convenience, and usability of AI-powered customer service systems.

Technology adoption has a relational and affective dimension of Trust Theory (McKnight et al., 2002). In addition to being functional, users should feel that the system and the institution that owns it is trustworthy, sincere and able to safeguard their interests. The level of trust is particularly important when it comes to matters of money transactions and personal information. The uncertainty and perceived vulnerability caused in the interaction between humans and AI can be mitigated through the use of trust in the case of banking chatbots.

Privacy Calculus (Culnan and Armstrong, 1999; Dinev and Hart, 2006) views the process of decision-making of a user as a trade-off between the perceived benefits and perceived risks of disclosure of data. Users determine the level of convenience and personalization of a system to be more important than the risk of losing control over personal information. This paradigm is especially applicable to millennials who are digitally active, as well as more informed about the dangers of data privacy.

These three perspectives make a multidimensional comprehension of the adoption of chatbots when combined. TAM describes the perceived usefulness and ease of use factors; Trust Theory describes the interpersonal and the institutional confidence factors; Privacy Calculus describes the risk perception and data sensitivity factors. A combination of them sheds light on how functional value, emotional assurance and ethical consideration all apply together to influence the behavior of users. The following section elaborates on how these theoretical foundations are operationalized through the key constructs examined in this study.

1.3 Theoretical Background of Key Constructs and Study Variables

This study examines how data privacy concerns affect millennial trust and online banking AI chatbot use intention in online banking. These are analyzed using several central constructs: data privacy concerns, trust in artificial intelligence systems, intention to use, perceived risk and usefulness, human-likeness, and previous experience in similar technology.

1.3.1 Data Privacy Concerns

Data privacy concerns imply the personal perception of fear or concern on the manner in which personal data is gathered, handled, stored and possibly made available to others (Culnan and Armstrong, 1999). In the financial services sector, the issues are particularly acute, as the clients are required to provide extremely sensitive data, including account numbers, transaction history, and personal identifiers, to the online services, including AI-based chatbots. Data privacy is threatened, which can make users unwilling to fully use digital services, especially when the problem of large-scale breaches of data and the misuse of algorithms is in the limelight (Hasal et al., 2021).

Chatbots in online banking can serve as the middle ground between the customer and the financial institution, and in many cases, the chatbot will be able to perform functions like balance

checks, payments, or even credit applications. Since these activities demand much input of information, the perception of millennials towards privacy protection may directly affect their readiness to use these systems. The digital literacy rates of millennials remain high, but the sensitivity of their personal and financial information remains high when it comes to how this data is handled. It has been established repeatedly that perceived risks that are associated with data handling, biasness of algorithms, or sharing information without authorization may be a major deterrent to this group to adopt AI systems in the banking sector (Bouhia et al., 2022; Giordani, 2023).

A number of studies give evidence to this effect. Lappeman et al. (2022) discovered that the perceived protection and transparency of the financial institutions played a crucial role in whether millennials went ahead and shared their personal information with banking chatbots. Equally, Hasal et al. (2021) affirm that explicit privacy policy, transparency in chatbots, and lack of past data breaches are some of the contextual indicators that affect the degree of trust and adoption intentions among users. The findings can be uniformed with Privacy Calculus Theory which holds that consumers compare the perceived advantages of a service (e.g., convenience, personalization) with the perceived threats to their privacy (Culnan and Armstrong, 1999).

Data privacy concerns can therefore be considered a focal independent variable in this research, as they directly influence user trust and indirectly affect the intention to use AI chatbots in online banking (Dinev & Hart, 2006; Luo et al., 2021). When users perceive that their personal information is handled securely and transparently, their level of trust increases and perceived risk decreases, which enhances their likelihood of continued or repeated use (Culnan & Armstrong, 1999; Lappeman et al., 2022). Conversely, insufficient protection of privacy rights or a lack of clarity regarding data-handling practices can heighten user skepticism and reduce willingness to engage with chatbot services (Beldad et al., 2011; Martin & Murphy, 2017).

Although the adoption of AI in banking is becoming a more popular topic of scholarly attention, there is still a gap in specific studies that can explore how various aspects of the data privacy concerns influences the perception of trust in AI chatbots. A significant part of the literature addresses the issue of privacy as a unit or concentrates on the security aspect without discussing the psychological aspects of security (Giordani, 2023; Lappeman et al., 2022). This research fills that gap by determining the particular aspects of the data privacy concerns, i.e. perceived data control, transparency, and institutional credibility, that affect the trust of millennials and, consequently, their desire to use AI chatbots within online banking applications.

1.3.2 Trust in AI Systems

One of the key concepts of comprehending technology acceptance and further use is trust. It is usually described as the disposition of one side to be susceptible to the behavior of the other on the understanding that the other would carry out a specific act that is significant to the trustor (Mayer et al., 1995). Trust is even more important in digital financial services where people are sharing personal and financial information, which is highly sensitive. Trust in online banking chatbots includes two main aspects institutional trust (belief in the bank as an entity) and technology trust (belief in the chatbot as a technological device) (Lappeman et al., 2022; Luo et al., 2021).

Some researchers note that trust plays a significant role in the use and further utilization of banking chatbots. Lappeman et al. (2022) proved that the perception of the integrity of the bank and the technological reliability of the chatbot largely determine the willingness of millennials to share personal information with the banking chatbots. The same findings were drawn by Luo et al. (2021), who concluded that the lack of trust in the bank and the chatbot infrastructure is the key to winning over the reluctance associated with privacy. Motivation According to Alagarsamy and Mehrolia (2023), millennials require to have secure authentication, clear communications, and human-like understanding to develop the needed trust to communicate with chatbots, as both technical and relational cues should be trusted, according to the authors, as the building blocks of trust.

Trust has also been identified to lead to a decreased perceived risk thus demonstrating more propensity to use AI chatbots. Shaikh et al. (2023) and Rohit et al. (2025) show that the role of trust in the banking industry is where privacy concerns and perceived risk and behavioral intentions are mediated by trust. High level of trust leads to low perceived risk and high behavioral intention. In contrast, in case of low trust, even small privacy or system failures may have a profound negative impact on the disposition to use the technology. This is in line with the Trust Theory, which holds that adoption can be achieved when the user perceives that a system is competent, reliable and behaves in a manner of integrity (Mayer et al., 1995).

Although the literature on the topic is increasing, comparatively few researchers have directly tested the mediating effect of trust in regard to data privacy concerns and the desire to use AI chatbots in internet banking. Majority of the previous literature considers trust as a result or anticipator without a discussion of its mediating and moderating position (Luo et al., 2021; Rohit

et al., 2025). The thesis fills this gap by modeling trust as one of the mediating variables, which is at the core of comprehending how the perception of millennials on the data privacy concerns can be transformed into a behavioral intention to use AI chatbots

1.3.3 Perceived Risk and Perceived Usefulness

Perceived risk is the estimation by an individual of the negative aspects and the elements of uncertainty of technology usage (Featherman and Pavlou, 2003). The perceived risk in the case of online banking chatbots is a range of concern related to data breaches, identity theft, technology-related errors, and personal information misuse. On the other hand, the perceived usefulness refers to the extent to which one considers the use of a given system to increase his or her performance or to allow an individual to perform better (Davis, 1989). These two constructs combined are vital elements of the Privacy Calculus as, when evaluated by users, the value of technology (usefulness) should be weighed against the potential negative impacts (risk) and then decide whether to use or not.

The study of AI chatbots in banking consistently demonstrates that considerable usefulness may not compensate formidable risk opinions. Mehrolia et al. (2023) discovered that perceived risk is an intermediate variable between customer satisfaction and sustained use of banking chatbots, which suggests that perceived risk may undermine even positive experiences. Similar results were reported by Hasan et al. (2023) who stated that the perceived risk reduces the intention to use conversational assistants in the banking sector, particularly when financial information is used. The results highlight that risk perception could be a key obstacle to the continued use of AI chatbots even by digitally competent millennials

Perceived usefulness, in its turn, is a dependable positive predictor of intention to use financial technologies all the time. Toh and Tay (2022) revealed that perceived usefulness has a considerable influence on the adoption of banking chatbots by millennials in the Malaysian context, and Thanh and Linh (2024) have shown the same in Vietnam. The study by Lubbe et al. (2025) found that the perceived usefulness chatbots can lead to further usage in millennials living in emerging markets, implying that usefulness can help to overcome a number of risk-related concerns.

These constructs act as contradictory forces to millennials: perceived usefulness is what drives them to use chatbots whereas perceived risk inhibits or mediates such use. This process

is consistent with the Privacy Calculus Theory (Culnan and Armstrong, 1999) that functions as a sociological theory that theorizes technology use decisions as a trade-off relationship between an expected reward and a perceived cost. Strong perceived risk that is lowered by high usefulness and strong institutional assurances (security, transparency), and higher intention to use may in turn be followed by a stronger intention to use. On the other hand, perceived risk and usefulness can be increased and a negative effect of usefulness negated with weak assurances or past negatively connoted experience.

Even though previous findings have explored the variables that determine AI chatbot adoption in the banking industry in-depth, most of the available studies have treated perceived usefulness and perceived risk as autonomous and independent variables in predicting behavioral intention. Technology Acceptance Model (TAM)-based research largely concentrates on the role of the perceived usefulness and ease of use in a direct antecedent of adoption (Davis, 1989; Venkatesh and Davis, 2000), whereas research based on risk and privacy literature concentrates more on perceived risk, data security or privacy concerns as obstacles to use (Featherman and Pavlou, 2003; Hasan et al., 2023). Nevertheless, there are theoretical approaches like Privacy Calculus Theory which postulates that decisions to adopt technology are not made as a result of single-factor analysis but rather as a thoughtful trade-off among the perceived maximum benefits and the perceived maximum risks (Culnan and Armstrong, 1999; Dinev and Hart, 2006).

This trade-off is particularly acute in the case of AI chatbots, where users are at the same time comparing the practical utility of chatbots (e.g., their efficiency, convenience, and saving time) with the possible risks of data misuse, privacy violation, and impossibility to control their personal financial data. It was empirically proven that high perceived usefulness is not always followed by adoption when perceived risk is high, especially in the area of financial services where the level of trust and the sensitivity of data are paramount (Mehrolia et al., 2023; Shaikh et al., 2023). On the other hand, risk perceptions can be reduced by strong institutional protection and perceived utility, which recommends an interdependent and not an independent relationship between the two constructs.

Regardless of these theoretical suggestions, the number of studies that empirically combine perceived usefulness and perceived risk into one unified model of AI chatbot adoption in banking is very low, particularly among millennials. This research is able to fill this gap by conducting a combined analysis of perceived usefulness and perceived risk on an integrated platform based on TAM and Privacy Calculus Theory, including the mediating factor of trust. In

this way, the research would be able to consider that the intention of millennials to use the AI chatbots in online banking is the result of a dynamic consideration of both the functional advantages and the psychological risks, but not of the evaluation of one or the other of these constructs in isolation.

1.3.4 Human-Likeness

Human-likeness, also known as anthropomorphism, is a measure of how non-human system like an AI chatbot behaves, speaks and looks like a human being (Epley et al., 2007). Human-likeness in the case of online banking may take the form of natural flow of conversation, empathic tone, responses that are personalized or even the capability to pretend to be emotionally understanding. All these characteristics are aimed at making the relationships with AI systems more exciting, intuitive, and socially significant (Sfar et al., 2025).

Conceptually, human-likeness is directly connected with the Social Presence Theory that assumes that the warmer and more inter-personally expressive a technology is, the greater the user will feel that he or she is socially connected and trusted (Short, Williams and Christie, 1976). Natural dialogue chatbots, those that appear to have an understanding or provide personalized help are more likely to boost perceived social presence and satisfaction and thus lead to the desire to repeat the experience. As an example, Sfar et al. (2025) showed that anthropomorphic signals, including the use of first-person pronouns, empathy, or the imitation of the conversational tone, increase user trust and desire to use AI chatbots in the financial sector.

The influence of human-likeness is not, however, a one-way effect. Surveys prove that too much anthropomorphism can cause the question of manipulation, data tracking, or even dishonesty, especially in such sensitive situations as banking (Ng et al., 2020). This effect is related to the uncanny valley effect, which states that excessively anthropomorphic technologies may provoke uneasiness or suspicion. Therefore, human-likeness in moderate degrees can frequently work best in establishing trust as opposed to highly realistic or emotive design.

Empirical research demonstrates that as chatbots have the right to be human-like, people tend to view them as more competent, relatable, and trustworthy (Alagarsamy and Mehrolia, 2023; Rohit et al., 2025). The digital-focused millennials can be positively affected by these features provided that they are aligned with the expectations of authenticity and data security. However, in other cases, when the human-like features appear to be overstated or intrusive, they can increase the privacy concerns and, in particular, the storage and analysis of conversational information (Ng et al., 2020).

Thus, human-likeness is operationalized as a moderating factor in this research to be strengthening or weakening the impact of data privacy concerns on trust. The moderate level of anthropomorphic qualities should eliminate negative concerns about privacy and lead to trust, unlike unreasonable human mimicking, which can make people more suspicious and unwilling to cooperate with chatbots in internet banking.

1.3.5 Prior Experience with digital technologies in general

Prior experience is the overall knowledge of digital technologies, systems that use artificial intelligence and online self-service platforms by users whose previous experience involves non-chatbot or non-banking interactions (Gefen, 2000). This experience influences the expectations of users, lessens uncertainty and allows the development of mental models as to how intelligent systems ought to work. When it comes to online banking, information on the previous experience with digital platforms, automated services, and AI-supported applications can contribute to the attitudes and responses of users to banking chatbots during the initial interaction.

According to Expectation-Confirmation Theory (ECT), such presumed experience in technology influences the behavioral intention through the development of confidence, expectations and the perceived control in the mind even before an individual accesses the particular system (Bhattacherjee, 2001). The more experienced users are in utilizing digital services, the more confident and less anxious they are likely to be when they come in contact with new technologies, as the less experienced ones can experience more uncertainty and risk. This process is especially applicable to the financial services industry where perceived complexity and sensitivity of data may increase the resistance experienced by the new systems.

The same view is in line with Trust Transfer Theory, which assumes that the trust formed under common technological systems can be obtained to new but related systems (Kim et al., 2008). In this regard, users who have already experienced any of the credible digital or AI-based services may feel more willing to rely on the chatbots as the initial point of contact in banks despite having no prior experience with chatbots. On the contrary, those users who have little experience with advanced digital technologies can be more skeptical and more concerned with privacy.

The importance of the general technological experience is backed up by empirical research as a factor of trust and intention. The studies show that more digitally literate users and those who were previously exposed to automated systems are more likely to report a lower

perceived risk and more willing to use AI-based services (Luo et al., 2021). Likewise, Lubbe et al. (2025) also note that positive experiences of digital self-service technologies lead to confidence and less resistance to new AI solutions, despite the situation being new.

Prior experience is thus in this paper conceptualized as a moderating variable which intervenes the extent into which data privacy concerns have an impact on trust in AI chatbots in a first-time use. It can be assumed that users who have a higher general technological experience will feel that there are less threats associated with privacy and will show a higher degree of initial trust whereas a user with a low level of experience may have a higher degree of privacy concerns and lower trust. This difference is especially relevant when one is looking at first-time intention to use AI chatbots in online banking among the millennials

1.3.6 Perceived Ease of Use

The Perceived Ease of Use (PEOU) is one of the key constructs of the Technology Acceptance Model and describes how much one believes that the use of a given system involves very little effort (Davis, 1989). In the case of the AI chatbots used in online banking, the perceived ease of use represents the ratings of the users regarding the intuitiveness, intelligibility, and ease of the experience with the chatbot, such as how easy it is to navigate, how understandable the responses are, and whether it involves any technical complexity.

Ease of use in digital banking contexts is a crucial factor when it comes to creating attitudes and trust towards the services of AI-based banking. Users who perceive the chatbots in the banking industry as user friendly have less cognitive load and feel less anxiety and this boosts their trust in the system (Venkatesh and Bala, 2008). In the case of millennials in particular, who are used to convenient and easy online interactions, complex interfaces or vague replies of chatbots can lead to frustration and a reduction in their desire to use the technology (Toh & Tay, 2022).

There is consistent empirical evidence that the perceived ease of use has a positive impact on trust and behavioral intention in situations of technology adoption. As Thanh and Linh (2024) discovered, the ease of use had a strong positive impact on the acceptance of e-banking chatbots by the millennials because the customers were willing to use the chatbots once they perceived the interaction as intuitive. Likewise, Giordani and Ferreira (2023) demonstrated that systems perceived to be user-friendly develop trust due to an indication of technological capability and dependability, particularly in financial services where users are very critical of mistakes and misconceptions.

Furthermore, the perceived ease of use is in close interaction with the perceived usefulness. It is also postulated by TAM that simple systems are better perceived as useful since users tend to accomplish their objectives efficiently without the need to make efforts that are avoidable (Davis, 1989). Within the framework of AI chatbots, the relationship implies that the intuitive conversational design creates a higher functional value and user satisfaction, which increases intention to use.

In this theoretical and empirical support, the concept of perceived ease of use in this paper is considered one of the antecedents of trust and intention to use AI chatbots in online banking, which can also be seen as a complement to perceived usefulness, and in this regard, the expectations of the usability of millennial users to these applications are considered.

1.3.7 Intention to Use

One of the most frequently studied constructs in the research on the technology adoption is behavioral intention, also commonly known as intention to use. The Technology Acceptance Model (TAM) defines intention to use as the willingness or the readiness of a person to use a certain technology and intention to use is the most immediate predictor of actual use (Davis, 1989). In the banking online banking setting, intention to use is the most suitable capture of the probability of millennials opting to use AI-powered chatbots to perform financial activities like checking account balances, transfer funds, or seek financial advice.

The research findings have repeatedly indicated that intention to use is affected not only by the instrumental factors (e.g., perceived usefulness and ease of use) but also by the psychological ones (e.g., trust and perceived risk). Shaikh et al. (2023) revealed that the intention of the customers to use chatbots in the banking industry is determined by the efficiency and convenience of the technology, as well as their customer perceptions of security and privacy. In a similar manner, Mehrolia et al. (2023) found that perceived risk mediates the relationship between user satisfaction and continued use, indicating that even satisfied users may discontinue usage when they perceive threats to privacy or security.

When it comes to millennials, the desire to use banking chatbots, specifically, outside the initial adoption, depends largely on the perception that the chatbot would be timesaving, reliable, and personally relevant. Toh and Tay (2022) established that perceived usefulness is a significant factor that influences millennials acceptance of banking chatbots in Malaysia as it poses as one of the factors at the adoption stage. By contrast, the case of Lubbe et al. (2025) indicated that

customer satisfaction and favorable digital experiences are the central factors when it comes to using chatbot-based services again, constituting post-adoption reviews as per existing usage experience. Such results are similar to the Privacy Calculus viewpoint that argues that millennials evaluate the advantages of chatbots (e.g., immediacy, personalization, and efficiency) against possible privacy and safety threats when they form their intention to use or not to use the technologies (Bouhia et al., 2022).

The role of trust in changing positive perceptions into behavioral intention is of special significance. With high trust, the perceived risk attributed to chatbots reduces, and more likely, a strong intention to use will develop in millennials. On the other hand, distrust can undermine intention to use even in case the technology is very functional or efficient (Shaikh et al., 2023; Rohit et al., 2025). Therefore, the intention to use is the dependent variable in the study since this variable entails the final behavioral finding of the millennial perception of data privacy, trust and the mediating variables of human-likeness and previous experience.

Although there has been increasing literature on the fintech and AI in banking, there have been limited studies which have modeled intention to use as an endpoint of a privacy trust mechanism. Most previous studies consider the functional drivers of intention to use but fail to speculate properly on the psychological and ethical aspect especially the data privacy concerns. This paper fills this gap by combining TAM and Trust Theory and Privacy Calculus Theory to determine the impact of privacy concerns in promoting trust and the latter in promoting the intention among millennials to use AI chatbots in online banking systems.

1.4 Understanding Millennial Users and Their Digital Behavior, Fintech Adoption and Privacy Attitudes

The term Millennials when broadly understood to denote people born in the year 1981 to 1996 is a very important demographic in the adoption of AI-driven services in the banking industry. As digital natives, this generation has been exposed to the fast-paced technological change and exhibit a high degree of familiarity and ease with online platforms (Uddin et al., 2024). Consequently, a sense of convenience, immediacy, and smooth digital experiences influences their financial practices with an anticipation of those experiences to match their overall lifestyle practices.

Millennials are known to use smart phones and mobile applications to carry out their daily lives including money matters. It is postulated that this group has more demands on 24/7 access, user-friendly design, and personalized services, compared to older generations (Lubbe et al., 2025). Suhartanto et al. (2022) observed as an example that in Indonesia, millennials were more likely to become loyal to AI-enabled banking systems when digital solutions did streamline process information in the process of performing their daily banking duties. Equally, Yussaivia et al. (2021) noted that the introduction of AI functions that improved convenience and efficiency had a strong effect on the adoption of the Islamic mobile banking by millennials.

One more distinctive aspect of millennial digital behavior is that they are ready to explore new technologies, but they should prove their value (Toh and Tay, 2022). Millennials are faster adopting financial technologies (fintech) including mobile banking apps, robo-advisors, and AI chatbots than the Generation Y (Ahamed et al., 2024). Nevertheless, they are not as enthusiastic as they critically assess risks, in particular, privacy and trust (Pelote, 2022).

The use of fintech (AI chatbots, in particular) by millennials can also be described in terms of models like the Technology Acceptance Model (TAM), in which perceived usefulness and ease of use are key factors. Empirical research supports this: Thanh and Linh (2024) found out that the perceived ease of use is an important factor affecting the adoption of e-banking chatbots in younger Vietnamese new customers. Similarly, Limakrisna and Moeins (2024) revealed that the further usage of chatbots by Indonesian millennials was determined by the total satisfaction with efficiency in services.

Moreover, the usage of fintech by millennials has a close connection with social influence and peer pressure. The study conducted by De Cicco et al. (2020) revealed that the attitude of millennials towards chatbots is determined not only by the perception of utility but also by the wish to preserve social conformity in the environment with the technological progress. This underscores the dual nature of personal utility and social validation in motivating the millennial fintech behaviors.

Although they are receptive to the use of digital banking tools, millennials also say they are more concerned about security and privacy of their data. According to Pelote (2022), privacy perceptions greatly influence the intentions of millennials to use AI in internet banking, where most of them consider perceived benefits against the risks of possible misuse of the data. As stated by Lappeman et al. (2022), the readiness of millennials to share personal data with banking

chatbots is subject to the intensity with which the respective institution expresses trust in the transparent and safe practices of data sharing, the following section focuses on trust in AI systems and its importance in shaping millennials' intention to use banking chatbots.

1.5 Summary of Key Constructs and Their Theoretical Basis

It is important to first generalize the relationship between the key constructs covered in the previous sections before displaying the summary table in the conceptual background of the study. All the constructs are based on either one or a combination of the three underlying theories; the Technology Acceptance Model (TAM), the Trust Theory, and the Privacy Calculus Theory: data privacy concerns, trust, intention to use, perceived risk, perceived usefulness, perceived ease of use, human-likeness, and prior experience. These constructs are summarized as presented in the following table with their theoretical definition, theoretical impacts on the conceptual model, and the main academic references that contribute to their consideration. This summary can be used to clearly understand the role played by each factor in explaining the trust and intention of millennials to use AI chatbots in online banking, Below, the table of key construct examined in this study, alongside their definition, role in the conceptual model and supporting literature are summarize in table 1

Table 1 Key Constructs of the Study and Their Role in the Conceptual Model

Factor / Construct	**Definition**	**Influence / Role in the Conceptual Model**	**Key Author Citations**
Data Privacy Concerns	Anxiety or apprehension about sharing personal and financial data online, especially with AI-driven systems.	Independent variable: directly and negatively affects trust; indirectly (through trust) affects intention to use.	Bouhia et al. (2022); Hasal et al. (2021); Giordani (2024); Lappeman et al. (2022)

Table 1 continuation

Trust in AI Systems (Institutional and Technology Trust)	Belief that the bank and the chatbot are competent, secure, and act in the user's best interests. Includes institutional trust (bank) and technology trust (chatbot interface).	Mediating variable: bridges data privacy concerns and intention to use.	Mayer et al. (1995); Lappeman et al. (2022); Luo et al., (2021); Alagarsamy & Mehrolia (2023); Rohit et al. (2025)
Perceived Risk	The perceived likelihood of negative consequences (data misuse, malfunction) from using AI chatbots.	Moderating variable: weakens the positive relationship between trust in AI chatbots and intention to use under conditions of high perceived risk.	Featherman & Pavlou (2003); Mehrolia et al. (2023); Hasan et al. (2023)
Perceived Usefulness (PU)	The degree to which using the chatbot improves banking efficiency and convenience.	Positive direct effect on intention to use	Davis (1989); Toh & Tay (2022); Lubbe et al. (2025); Thanh & Linh (2024)
Perceived Ease of Use (PEOU)	The extent to which using the chatbot is free of effort.	Positive direct effect on intention to use; interacts with PU.	Davis (1989); Toh & Tay (2022); Thanh & Linh (2024)
Human-Likeness (Anthropomorphism)	The extent to which a chatbot mimics human traits (natural conversation, empathy, personalization).	Moderating variable: can enhance or weaken the effect of privacy concerns on trust and trust on intention to use.	Sfar et al. (2025); Ng et al. (2020)

Table 1 continuation

Prior Experience	Users' previous interactions with similar technology.	Moderating variable: experienced users in similar technology feel less risk and higher trust; moderates privacy concerns → trust relationship.	Luo et al. (2021); Lubbe et al. (2025)
Intention to Use AI Chatbots	The degree to which millennials are ready and willing to use AI chatbots for online banking tasks.	Dependent variable: predicted by perceived usefulness, perceived ease of use, trust, and moderated by perceive risk.	Davis (1989); Shaikh et al. (2023); Mehrolia et al. (2023); Toh & Tay (2022); Lubbe et al. (2025)

Source: The table was compiled by the author.

The literature reviewed indicates that trust is key in the determination of the adoption and continuation intentions especially in digital financial setting where there is uncertainty and perceived risk (Gefen et al., 2003; McKnight et al., 2011). The data privacy concerns prove to be one of the most problematic precursors of trust because the problems of data gathering, processing, and storage of personal and financial information have a detrimental effect on the confidence of users both in the technology itself and the institution delivering it (Dinev and Hart, 2006; Martin et al., 2017). Meanwhile, the perception of usefulness and the perception of ease of use still continue to be the underlying forces of technology acceptance, which aligns with the Technology Acceptance Model since users would tend to develop positive attitudes to the AI chatbots, when they regard them as effective, convenient, and easy to communicate with (Davis, 1989; Venkatesh and Davis, 2000).

The Privacy Calculus Theory adds on this by stating that users possess cognitive balancing of the advantages of using AI chatbots against the possible threats to privacy and security and then have their behavioral intentions (Culnan and Armstrong, 1999; Dinev et al., 2006). In this mechanism, trust is the mediating variable that converts the perception of privacy and risk to intention to use or persist to use AI chatbots, which implies that the positive

impressions of trust may partially counter privacy related concerns (Pavlou, 2003). Further, the existing literature suggests that the perceived risk can negate the positive impact of usefulness and trust on adoption decision, and this suggests that risk management and open data-handling practice can be critical in financial services (Featherman and Pavlou, 2003). Additional factors that affect the impact of privacy concerns on the user and the design, including previous experience with similar systems and the extent of anthropomorphic human-likeness, also contribute to the effect of privacy concerns on trust, with familiarity and properly implemented anthropomorphic qualities potentially diminishing uncertainties, whereas too much anthropomorphic qualities or lack of experience can enhance perceived risk (Lankton et al., 2015; Aarujo, 2018).

Overall, the literature presents millennials as users with high tech savvy but privacy-conscious who constantly have to juggle efficiency, convenience, and ethical considerations regarding the data protection when using AI-based financial services (Bolton et al., 2013; Buck and Wojdynski, 2016).

The coherence of functional, psychological, and ethical aspects makes the integrated theoretical framework a systematic basis of the formulation of hypotheses and conceptual research model used in this study, which is developed based on the Technology Acceptance Model (TAM), Trust Theory, and Privacy Calculus Theory, and empirically tested in the following chapters.

2. METHODOLOGY OF TRUST AND DATA PRIVACY CONCERNS IN THE USE OF AI CHATBOTS IN ONLINE BANKING

2.1 Research model, aim and hypothesis

In this part, the effects of data privacy concerns on trust and intention to use AI chatbots in online banking are addressed. Based on literature review, the most applicable variables that can be used to reflect the technological and psychological antecedents of chatbot usage were chosen: the data privacy concerns (Dinev and Hart, 2006; Luo et al., 2021), perceived usefulness (Davis, 1989; Lappeman et al., 2022), perceived ease of use (Venkatesh and Davis, 2000), and perceived risk (Beldad et al., 2011). The reason why these antecedents are selected is that they are the most important variables concerning the trust and behavioral intention toward technology in online financial services.

Also, moderating variables are human-likeness (anthropomorphism) and previous experience which can either contribute to the effect or weaken the effect of privacy concerns on trust. The mediating variable is the variable trust in AI chatbots, which is considered to be at the center of the privacy concerns and intention to use as the central aspect of technology adoption and trust in their use.

Aim of the Empirical Research:

The aim of the empirical research is to collect and analyze quantitative data to assess the influence of data privacy concerns**,** technology acceptance factors, and risk perceptions on trust and intention to use AI chatbots in online banking among millennials.

Objectives of the Empirical Research:

1. To develop a conceptual research model and formulate hypotheses integrating the Technology Acceptance Model (TAM), Trust Theory, and Privacy Calculus Theory in the context of AI chatbot use in online banking.
2. To identify the key factors influencing millennials' trust and intention to use AI chatbots in online banking.
3. To empirically test the effects of data privacy concerns, perceived usefulness, perceived ease of use, and perceived risk on trust and behavioral intention.

4. To analyze the mediating effect of trust in the relationship between data privacy concerns and intention to use AI chatbots.
5. To evaluate the moderating effects of human-likeness and prior experience on the relationship between data privacy concerns and trust.
6. To interpret the results and provide recommendations for improving trust and adoption of AI chatbots in the banking context.

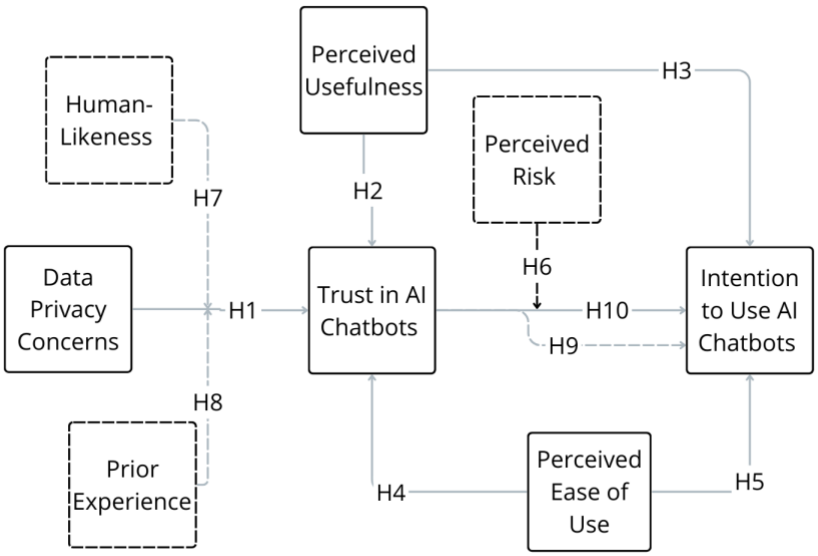
Research Model

The research model was developed based on an integration of the **Technology Acceptance Model (TAM)** (Davis, 1989; Venkatesh & Davis, 2000), **Trust Theory** (McKnight et al., 2002), and the **Privacy Calculus Model** (Dinev & Hart, 2006).

In this model:

- Data Privacy Concerns**,** Perceived Usefulness**,** and Perceived Ease of Use are the independent variables.
- Trust in AI Chatbots is the mediating variable, connecting privacy and technology perceptions with behavioral intention.
- Human-Likeness and Prior Experience are the moderating variables influencing the relationship between Data Privacy Concerns and Trust
- Perceived Risk is the moderating variables influencing the relationship between Trust and the Intention to use AI chatbots in online banking.
- Intention to Use AI Chatbots is the dependent variable, representing users' likelihood of adopting or continuing to use the technology.

Figure 4. Research model



Source: The figure was compiled by the author.

Hypotheses to Be Tested in the Empirical Study

Data privacy concerns can be defined as the feeling of vulnerability by the users on the way their personal data is handled, gathered, and stored by the digital systems. Privacy is one of the key determinants of trust in online banking where sensitive financial information is exchanged. According to preliminary findings, a high level of privacy can severely reduce the level of trust that people have on the internet-based technologies because people might suspect that someone may abuse their data or even give it to a third party (Dinev and Hart, 2006; Culnan and Armstrong, 1999). In particular, when it comes to the AI chatbots, the lack of transparency concerning data collection and processing is the key to alleviating the perceived risks to a greater extent and building confidence (Luo et al., 2021). Users will trust the technology more when they feel that the chatbot of their bank-related information is functioning safely. On the other hand, the perceived inability to control or bad data management lowers trust and prevents engagement. Based on this, the following hypotheses has been raised:

H1: Data privacy concerns negatively impact Trust in AI chatbots.

Perceived Usefulness can be defined as the level, at which a person feels that the usage of a certain system can improve his or her performance (Davis, 1989). Applicability, when applied

to online banking, can be considered as how much AI chatbots are useful to users in terms of making their financial services more effective, e.g. faster in service interaction, direct, or easier in account management. The past studies have always indicated that when the users see a technology useful, then they tend to trust the system more. Research conducted by Venkatesh and Davis (2000) and Giordani and Ferreira (2023) revealed that the perceived usefulness makes a significant contribution to enhancing the trust of users in the digital financial tools. Based on this, the following hypotheses has been raised:

H2: Perceived Usefulness positively impacts Trust in AI chatbots.

There is also a direct and well-developed impact of Perceived Usefulness on behavioral intentions of the users. As per the TAM studies, people are ready to develop and maintain the use of a technological system when they feel that it has a significant positive impact on their work (Davis, 1989; Venkatesh and Davis, 2000). Millennials in an online banking setting tend to apply AI chatbots more when they believe that it comes with a distinct functional benefit, e.g., faster response times or higher convenience or automation of their tasks. Empirical research indicates that an increasing perceived usefulness results in the increase of an intention to use AI-driven financial services (Giordani and Ferreira, 2023; Lappeman et al., 2022). Based on this, the following hypotheses has been raised:

H3: Perceived Usefulness positively impacts the Intention to Use AI chatbots in online banking.

Perceived Ease of Use is understood as a degree of how a person thinks that it takes little effort to operate a system (Davis, 1989). Within the framework of online banking, this is the extent to which the interface of the chatbot is intuitive, easy, and user-friendly. When communication with the chatbot is not complicated and involves no technical skills, users will have lighter cognitive load, fewer obstacles and less clumsy navigation. According to previous studies, ease of use will have a direct impact on developing trust in the use of digital tools because a user is more confident and less intimidated when the system is not complicated (Venkatesh & Bala, 2008). Therefore, millennials will have a better confidence in banking chatbots when they view them as easy to operate. Based on this, the following hypotheses has been raised:

H4: Perceived Ease of Use positively impacts Trust in AI chatbots.

Besides its role in influencing trust, Perceived Ease of Use is a well-established cause of behavioral intentions in other technology adoption settings. Studies, based on the TAM, show that where a system is simple to operate, people tend to have better chances of staying with it owing to the fact that the interaction process becomes comfortable and reachable (Gefen et al., 2003; Davis, 1989). To millennials, who often base their decisions on quick and painless online solutions, ease of use is the key factor in future follow-up on the use of AI chatbots when performing banking operations. The more pleasant the experience, the more chances of further adoption. Based on this, the following hypotheses has been raised:

H5: Perceived Ease of Use positively impacts the Intention to Use AI chatbots in online banking.

Perceived Risk reflects the ambiguity and the possibilities of bad things happening with the usage of a digital system (Featherman and Pavlou, 2003). Financial loss, information breach, or system failures may be considered as risks in online banking. In previous studies, it is observed that the perceived risk has the potential to diminish the correlated relationship between trust and intention to use because even highly trusting users might be too afraid to trust chatbots in case of a high risk of harm (Beldad et al., 2011). Hence, the perceived risk is supposed to mediate the trust - intention relationship, with the positive impact of trust on usage intention being less in the scenario where the perceived risk is high. Based on this, the following hypotheses has been raised:

H6: Perceived Risk moderates the relationship between Trust in AI chatbots and Intention to Use, such that the positive effect of Trust is weaker under high perceived risk.

Human-likeness is the degree to which a chatbot mimics human behavior in terms of conversational tone, empathy or natural interaction. The existing literature on anthropomorphism indicates that human-like interface promotes emotional attachment and user trust (Epley and Waytz, 2010; Sheehan et al., 2020). Nonetheless, there are also some fears regarding manipulation or privacy invasion, particularly in finances in case of over-anthropomorphism. Therefore, the human-likeness has the capacity to build or undermine the trust of users based on perceived authenticity and openness. Human-likeness is conceptualized in this study as a moderator, which strengthens the positive relationship existing between data privacy transparency and the creation of trust. Based on this, the following hypotheses has been raised:

H7: Human-Likeness moderates the relationship between Data Privacy Concerns and Trust in AI chatbots, such that higher human-likeness enhances the positive impact of transparent privacy handling on Trust.

Users may form trust in connection with the usage of similar AI or online banking technologies since it is possible to be predisposed to trust, even without interaction with AI. The knowledge of digital interface and data security systems is also more common in experienced users, and this lessens uncertainty, increases confidence in technology (Gefen et al., 2003; McKnight et al., 2002). Therefore, prior experience can buffer the association between data privacy concern and trust experienced users will be less concerned about privacy threats and more inclined to trust chatbots than users with minimal experience with such systems. Based on this, the following hypotheses has been raised:

H8: Prior Experience with similar technology usage moderates the relationship between Data Privacy Concerns and Trust, such that users with more experience perceive less privacy risk and greater Trust.

Trust in a digital setting is frequently a key moderator in the relationship between cognitive assessment (e.g. perceived risk or privacy concern) and behavioral intention among users. As postulated by Privacy Calculus Theory, the potential benefits and perceived risks make users choose whether to share information or not, or to interact with technology (Dinev and Hart, 2006). In instances where data privacy practices are clear and transparent, users will feel greater trust that will translate to greater adoption intentions. On the other hand, the lack of trust due to privacy concerns may undermine the will to employ chatbots, no matter how useful they may seem. This mediating role of trust in the relationship between privacy perceptions and behavioral outcomes supports the claim made by previous researchers (Beldad et al., 2011; Luo et al., 2021). Based on this, the following hypotheses has been raised:

H9: Trust in AI chatbots mediates the relationship between Data Privacy Concerns and Intention to Use AI chatbots.

The concept of trust is a central factor in the adoption of technology and especially in the adoption of risk-related areas like financial services. Trust enhances less uncertainty and allows users to trust automated systems in performing sensitive tasks. The previous research reveals that the trust of users in digital technologies has a positive impact on the behavioral intention to

implement and use it (McKnight et al., 2002; Lappeman et al., 2022). Trust in the example of AI chatbots will include the beliefs related to the competence, integrity, and reliability of the chatbot. Upon the perceptions of the users that a chatbot is capable of aiding the banking tasks in a secure and efficient manner, the chances of the latter to accept the service rise. Therefore, trust is a psychological assurance mechanism that helps users to make a decision to use chatbots. Based on this, the following hypotheses has been raised:

H10: Trust in AI positively influences the Intention to Use AI chatbots in online banking among millennials.

2.2 Data collection instrument

The author in the research seeks to examine the impact of data privacy issue on trust and the willingness to use AI chatbots in online banking websites among millennials. The study tool is a self-administered questionnaire that was given online and was utilized to gather quantitative information of the target population. The rationale behind this choice is that it is simple to administer, inexpensive, and best suited to digital native respondents since the millennials spend most of their time online and have no problems with filling out online surveys.

To make certain that the respondents have a similar understanding of AI chatbots, the questionnaire started with a short description of AI-powered chatbots and their common uses in online banking. The survey also included examples in form of scenarios to demonstrate the chatbot interaction in a real banking situation. The respondents were randomly chosen to be in one of the two scenarios that had a difference in the extent of chatbot human-likeness. In one of the scenarios, a chatbot with poor human-likeness like a robot, formal, system-oriented speech was shown whereas in the other scenario, the chatbot with high human-likeness like a human, conversational speech, personalization, and empathetic statements were presented. These are the only differences in style, the functionality and informational content of the two scenarios was the same.

After being subjected to the given scenario, the subjects rated a set of Likert-scaled statements, which assessed the data privacy concerns, perceived usefulness, perceived ease of use, perceived trust, perceived risk, and their intentions to use AI chatbots. By doing this, it was possible to test the hypothesis of human-likeness as a moderating variable and improve the realism and validity of the results in the context of the collected responses. The questionnaire was constructed with reference to the validated measurement scales applied in the past empirical

research in the directions of technology acceptance, trust, and data privacy. The products were a bit modified to suit the online banking environment.

The questionnaire (Annex 1) was based on the closed-ended questions, and all the constructs were assessed on five-point Likert scale between 1 (strongly disagree) and 5 (strongly agree). The reason why this scale was selected is that it is a scale that is easy to understand, it also avoids fatigue on the side of the respondent and gives enough variability to enable statistical analysis.

The structure of the questionnaire is as follows:

- **Part 1:** Introduction explaining the aim and purpose of the study, confirming confidentiality, and ensuring voluntary participation.
- **Part 2:** Screening questions are designed to verify that the respondent belongs to the target population: Millennials aged 29–40 who regular online banking users are and have not used an AI chatbot provided by a banking platform within the last 6 to 12 months**.** Respondents who do not meet these criteria (e.g., under 29 or over 40, rarely use online banking, or have previously used a banking AI chatbot) will be thanked for their interest and exited from the survey.
- **Part 3:** Questions measuring Data Privacy Concerns, including the perceived safety, transparency, and fairness of data handling.
- **Part 4:** Items assessing Perceived Usefulness and Perceived Ease of Use as defined by the Technology Acceptance Model (TAM).
- **Part 5:** Items measuring Trust in AI Chatbots, capturing users' perception of reliability, honesty, and competence.
- **Part 6:** Items related to Perceived Risk, Human-Likeness, and Prior Experience.
- **Part 7:** Questions capturing Intention to Use AI Chatbots in online banking.
- **Part 8:** Demographic information, including gender, country, education level, and occupation.
- **Part 9:** Closing statement expressing appreciation for the participant's time.

Each variable was measured using pre-validated scales from established research (Davis, 1989; Dinev & Hart, 2006; McKnight et al., 2002; Lappeman et al., 2022). The measurement structure, number of items, and expected reliability coefficients are presented in Table 2.

Table 2 Constructs Used in the Research, Measurement Items, and Reliability

Construct	Number of Items	Measurement Scale	Cronbach's Alpha (expected)	Source
Data Privacy Concerns	9	5-point Likert scale	0.807	Dinev & Hart (2006); Malhotra et al. (2004) Bellman et al. (2004); Beldad et al. (2011) Smith et al. (1996); Martin (2019)
Perceived Usefulness (PU)	4	5-point Likert scale	0.835	Davis (1989); Venkatesh & Davis (2000)
Perceived Ease of Use (PEOU)	4	5-point Likert scale	0.853	Davis (1989); Venkatesh & Bala (2008)
Trust in AI Chatbots	5	5-point Likert scale	0.784	McKnight et al. (2002); Lappeman et al. (2022)
Perceived Risk	4	5-point Likert scale	0.802	Featherman & Pavlou (2003)
Human-Likeness	4	5-point Likert scale	0.723	Epley & Waytz (2010); Sheehan et al. (2020)
Prior Experience	3	5-point Likert scale	0.788	Gefen et al. (2003)
Intention to Use	3	5-point Likert scale	0.870	Venkatesh & Davis (2000); Lappeman et al. (2022)

Source: Compiled by the author based on previous research findings.

2.3 Population and sample

The target population for this study consists of Millennials (aged 29–40) who have not interacted with AI chatbots in online banking within the last twelve months. Eligible participants include individuals who have used chatbots for account inquiries, transactions, or financial guidance through digital banking applications.

Given the online nature of the study and the difficulty of obtaining a complete sampling frame, a non-probability voluntary sampling method will be applied. This technique is appropriate because the target group is digitally active and easily reachable via online platforms such as Facebook, LinkedIn, and Instagram. The survey link will also be distributed through university mailing lists and financial-technology discussion groups.

To determine an adequate sample size, previous empirical studies on AI chatbot adoption, data privacy, and trust in online financial services were reviewed. The reported number of respondents in these studies is presented in Table 3.

Table 3 Previous Empirical Studies on Trust, Privacy, and Chatbot Adoption in Banking

Author(s) & Year	Research Context	Number of Respondents
Luo et al. (2021)	Trust and privacy in AI chatbot adoption for banking	312
Lappeman et al. (2022)	AI chatbots and customer experience in digital banking	278
Giordani & Ferreira (2023)	Trust, transparency, and privacy in AI-driven financial chatbots	241
Lubbe et al. (2023)	Building trust in conversational AI for financial services	198
Dinev & Hart (2006)	Privacy calculus in e-commerce adoption	162

Source: Compiled by the author based on published empirical studies.

All these studies have an average sample size of about 238 respondents.

Through this benchmark and with the scope of the research in mind, a target population of approximately 220 respondents is considered to be adequate to guarantee credible findings when relating, performing regression, and mediation/moderation analyses and still having statistical validity at 95% confidence level and a 5% error margin.

This is a sufficiently large sample, which will provide sufficient representation of the millennial user group, in addition to the fact that all key variables, such as the data privacy concerns, the perceived usefulness, the perceived ease of use, the perceived risk, the trust, the

human-likeness, the prior experience, and the intention to use is statistically powerful enough in terms of analysis.

2.4 Methods and statistics for data analysis

The primary data of this research will be gathered with the help of Google Forms as it will provide the opportunity to develop a proper survey and ensure safety in data storage. The answers will be exported and analyzed with the help of JASP. The JASP will offer a wide set of statistical functions used to analyze the connection between variables and test hypotheses of the study.

The analysis of data will be conducted in a number of steps. To begin with, data screening will occur in order to identify missing or inconsistent replies. Demographic data will be summarized using descriptive statistics (means, standard deviations, frequencies) and will be used to construct distributions. Cronbachs Alpha will be used in reliability analysis to determine if the internal consistency is good and factor analysis will be used to determine the validity of the constructs.

In order to test the hypothesis postulated, correlation and multiple regression will be done to test direct correlations between variables. The indirect effect of trust between the data privacy concerns and intention to use will be tested using mediation analysis, and the effect of perceived risk, human-likeness, and prior experience shall also be evaluated using moderation analysis. The level of statistical significance that will be tested is 0.05. The findings will be explained to give answers to behavioral and technological issues that affect millennials to adopt AI chatbots in web banking systems.

2.5 Ethical Considerations

Ethical integrity is the key point of the given study because the issues under discussion, which are data privacy and trust, are ethical by themselves. The study is based on the ethical guidelines of the research ethics committee of the university, and it meets all the requirements of the General Data Protection Regulation (GDPR, 2018). Electronic consent to partake in the study will be given to all participants by informing them of the intent of the study and its voluntary nature. No personal details will be gathered in the research and therefore the research results will be anonymous and confidential. The analysis of responses will be done aggregately, and they will be stored in password-protected files available only to the researcher and supervisor and destroyed permanently at the end of the project as per the university policy. The involvement will

be voluntary, and the respondents will have the freedom to pull out any time before they can submit their responses without any repercussions. The research does not present any physical, psychological or financial harm to the participants and any questions that may be considered sensitive in any way can be skipped without any restrictions. The principles of data minimization, purpose limitation, and confidentiality will be applied in the data handling in order to adhere to the standards of GDPR. Lastly, academic honesty will occur by properly, transparent, and honest reporting of the results and that all secondary sources will be referenced and credited.

3. DATA ANALYSIS AND REVIEW OF RESEARCH RESULTS

3.1 Demographic escription of participants

Through the online survey, the initial number of responses that were obtained was 298. Following the screening criteria that have been pre-determined, 221 valid answers were kept being examined further. The responses were not counted in the case participants were not included in the target group (millennials), rarely used online banking services, or stated that they were already using banking chatbots, as the research is intended to involve first-time users of online banking chatbots.

Table 4 shows the age distribution of the respondents. Of the valid respondents, the proportion of those within 29-34 age range (46.6%) was 139, and that between 35-40 age range (43.3%) was 129. This proves that the sample fits the target population of millennials that has been established in this study. The comparatively equal representation of the two age groups offers sufficient representation of younger and older millennials and makes the findings of the study relevant to the generation.

Table 4 Distribution of respondents by age.

What age group you belong to?	**Frequencies**	**Percentages**
29-34	139	46,6%
35-40	129	43,3%

Source: the figure was compiled by the author using the research results.

Table 5 provides an overview of the frequency of online banking use among the respondents. On eliminating the respondents who claimed to have used the online banking services rarely, 243 respondents survived this phase of screening.

The findings show that 31.75% percent of the participants have been using online banking services several times per week, and 24.6% percent used it daily. Moreover, 19.8% also use online banking once a week and 14.6% also use online banking several times a month. These results indicate that most of the respondents are frequent consumers of online banking services, which supports the appropriateness of the sample group when discussing the perceptions of AI chatbots in an online banking setting. In general, the findings verify that online banking has become a part of the daily financial lives of the respondents.

Table 5 Frequency of using an online banking service

How often do you use online banking services (app or website)?	**Frequencies**	**Percentages**	**Cumulative percentage**
Daily	66	24,6%	24,6%
Several times per week	85	31,7%	56,3%
Once per week	53	19,8%	76,1%
Several times per month	39	14,6%	90,7%
Rarely	25	9,3%	100%

Source: the table was compiled by the author using the research results.

The respondents who had interacted with a banking chatbot in the past were not included to make sure that the perceptions were based on the hypothetical first-time use scenario. Table 6 reveals that 22 respondents (9.1%) used a banking chatbot before, thus eliminated off the sample. The final sample comprised of 221 participants (90.9%) who answered “NO” as not used a banking chatbot, which was in line with the research design of the study.

Table 6 Previous use of banking chatbots

Have you used an AI chatbot provided by an online banking platform within the last 12 months?	**Frequencies**	**Percentages**	**Cumulative percentage**
No	221	90,9%	100%

Source: the table was compiled by the author using the research results.

Regarding prior experience with AI technologies not related to banking, the respondents were asked to answer whether they used other AI-based digital assistants in the past six months. The findings indicate that, 208 respondents (94.1%) said yes whereas only 13 respondents (5.9%)

said no prior experience. It indicates that the overall awareness of AI technologies among the participants is high and can be applied to explanation of the perceptions of trust, privacy, and adoption intentions in AI chatbots.

Table 7 Previous use of similar technology

Have you used other AI-based digital assistants (e.g., Siri, Alexa, ChatGPT, Google Assistant, e-commerce chatbots) in the last 6 months?	**Frequencies**	**Percentages**	**Cumulative percentage**
Yes	208	94,1%	94,1%
No	13	5,9%	100%

Source: the table was compiled by the author using the research results.

Table 8 demonstrates the gender distribution of the final sample. This sample was made up of 112 males' respondents (50.7%) and 106 females' respondents (48%) with 3 respondents (1.4%) choosing not to say. This comparatively equal gender representation enhances the potential of making generalizations of the results among the millennial generation. The ones which answered prefer not to say were considered as missing values in further analysis since they were almost minimal.

Table 8 Distribution of respondents by gender.

Gender	**Frequency**	**Valid percent**
Male	112	50,7%
Female	106	48%
Prefer not to say	3	1,4%

Source: the table was compiled by the author using the research results.

The respondents were also requested to specify the highest level of education accomplished and their current states of employment. Most of the respondents (45.2 %) had a master's degree as demonstrated in Table 9, then those who had a bachelor's degree (40.7 %).

A lower percentage had done Doctoral studies (11.3%), with 2.7% having high school level education. It means the sample possesses a rather high level of education, which is compatible with the frequent usage of digital banking services and AI technologies.

Regarding employment status, most respondents were employed (86%) with 14% indicating that they were self-employed. None of the respondents chose student or unemployed categories in the middle of the analysis. This pattern of employment indicates that most of these participants are economically active, which further supports the validity of studying privacy and trust perceptions with regards to income in online banking.

Table 9 Distribution of education level and employment status among respondents.

Variable	Categories	Frequency	Valid percentage
Education level	High school	6	2,7%
	Bachelor's	90	40,7%
	Master's	100	45,2%
	Doctorate	25	11,3%
Employment status	Student	-	-
	Employed	190	86%
	Self-employed	31	14%
	Unemployed	-	-

Source: the table was compiled by the author using the research results.

The participants were requested to state their monthly income, which was assumed to be approximately. Income distribution among categories as Table 10 indicates, was relatively well distributed with the highest percentages in the brackets of between €1,000–€1,999 and €2,000-€2999 per month. Less percentage of those who earned below €1,000 reported it whereas a significant percentage of those who earned above €3,000 chose it. Other respondents did not reveal their earnings, and their answers were considered to be missing data in further analysis.

This fact is evidenced by the diversity of the income levels in the sample, which makes the analysis robust since the views on the privacy risk and the trust in online banking can differ under various financial conditions.

Table 10 Distribution of income level among respondents.

Income level	Frequency	Valid percent
Less than €1,000	10	4,5%
€1,000–€1,999	89	40,3%
€2,000-€2999	69	61,2%
€3,000 or more	23	10,4%

Source: the figure was compiled by the author using the research results.

3.2 Reliability of instruments

The consistency of the measurement instruments was also measured in terms of Cronbach alpha which determines the internal consistency of multi-item constructs. All the constructs, as indicated in Table 11 (Annex 2), had values that were greater than the recommended value of 0.70, which denotes a good level of reliability.

Table 11 Cronbach' s Alpha coefficient

Construct		Numbers of statements	Cronbach's alpha from the original source	Cronbach's alpha in this research	Cronbach's alpha combined
Data Privacy Concerns	**Security (DPC-S)**	3	0,807	0,820	0,900
	Transparency (DPC-T)	3		0,766	
	Fairness (DPC-F)	3		0,765	
Perceived Usefulness		4	0,835	0,762	-
Perceived Ease of Use		4	0,853	0,824	-
Trust in AI Chatbots		5	0,784	0,811	-
Perceived Risk		4	0,802	0,796	-
Human-Likeness	**Scenario A (HL-A)**	4	0,723	0,693	0,812

Table 11 continuation

Human-Likeness	**Scenario B (HL-B)**	4		0,797	
Prior Experience		3	0,788	0,816	-
Intention to Use		3	0,870	0,864	-

Source: the table was compiled by the author using the research results.
Note: HL-A = Scenario A (High Human-Likeness) act more like a robot; HL-B = Scenario B (Low Human-Likeness) act more like a human.

The construct of Data Privacy Concerns had high internal consistency with its three dimensions; security (α = 0.820), transparency (α = 0.766), and fairness (α = 0.765). When the two were summed together, the total reliability of the data privacy construct was α = 0.900 which is excellent internal consistency.

Equally, Perceived Usefulness (α = 0.762) and Perceived Ease of Use (α = 0.824) were both of good reliability, as has been demonstrated in other studies involving Technology Acceptance Model (TAM). Internal consistency was also high in Trust in AI Chatbots (α = 0.811) and Perceived Risk (α = 0.796).

In case of the moderator Human-Likeness, Scenario A (highly human-like chatbot) had a slightly smaller Cronbachs alpha (α = 0.693) which is still acceptable for exploratory research. Scenario B (robotic chatbot) was more reliable (α = 0.797). The overall reliability of the construct was α = 0.812, the combined reliability score of human-likeness.

Lastly, Prior Experience (α = 0.816) and Intention to Use (α = 0.864) also had higher than appropriate reliability coefficients, indicating that the scales can be utilized when testing additional hypotheses.

Overall, it can be stated that all the measurement tools employed in the given study are valid and can be used in the further tests of validity and structural analysis.

3.3 Normality analysis

Since this study will have a sample size of 221 respondents, the Shapiro-Wilk test was applied to test the normality of the data. Based on the findings in Table 12 (Annex 3), the p-values in all cases were less than 0.05 and as such, normality could not be entirely accepted. Although

the normality test made the results, the analysis was proceeded. As the data collected in the 5-point Likert, the normality tests may not be all reliable particularly when the sample is large. Because of the significance of normal distribution in regression analysis, further analysis of skewness and kurtosis were conducted in the section of descriptive statistics.

Note: “Skewness and kurtosis are statistical measures that describe the shape of a data distribution. While skewness indicates the asymmetry of the distribution, kurtosis measures the heaviness of its tails compared to a normal distribution.”

Table 12 Tests of normality

Construct	Shapiro-Wilk		
	Statistic	df	Sig.
Data Privacy Concerns	0.907	221	< .001
Perceived Usefulness	0.895	221	< .001
Perceived Ease of Use	0.896	221	< .001
Trust in AI Chatbots	0.899	221	< .001
Perceived Risk	0.884	221	< .001
Human-Likeness	0.836	221	< .001
Prior Experience	0.839	221	< .001
Intention to Use	0.842	221	< .001

Source: the table was compiled by the author using the research results.

3.4 Descriptive statistics

8 constructs were studied in this research and their influence on intention to use AI chatbots in online banking. A 5-point Likert scale was used to measure all items of the construct. The constructs mean scores were as follows: 3.02-4.48 as the results are shown in Table 12 (Annex 4) which means that the judgment of the respondents was rather positive than negative.

The mean values cannot be used to draw concrete conclusions because no sampling error should be taken into consideration. Nonetheless, the descriptive statistics will give an idea of the broad perception of respondents. In examining the values based on the distribution of the data, all the skewness values of the constructs lie within the acceptable range, which is -2 to +2, and the values of its kurtosis also lie within or near the acceptable range. Thus, even though the previous findings of the Shapiro-Wilk test of normality show that the distributions are not normal

enough, the distributions may be taken as sufficiently normal and the assumption of the normality is valid to continue with the further parametric tests, such as the regression analysis.

The means provide the general indication of how the respondent perceptions are related to each of the constructs in the research. The increased mean scores indicate a greater level of agreement to the statements and indicate more positive attitudes to the corresponding construct, including increased perceived usefulness, increased trust, or increased intention of using AI chatbots. On the other hand, the one with low mean values shows less agreement and hence more concerns or reservations specifically on the data privacy concerns and perception risk.

The variations in the mean values of the constructs help to demonstrate how online banking users rank the different elements of using AI chatbots. As an illustration, the relatively high average scores regarding perceived usefulness and ease of use indicate that millennials tend to attribute AI chatbots as useful and simple to use. Conversely, the data privacy concerns, or perceived risk have a lower average, which means that there are different levels of fear about data security and its adverse effects. On the whole, the average figures give us an idea of the overall attitude trends of the respondents and serve as the context of the further inferential statistics.

Table 13 Comparison of means.

Construct	Mean	Std. Deviation	Skewness	Kurtosis
Data Privacy Concerns	4.472	0.440	-0.998	1.612
Perceived Usefulness	4.481	0.427	-0.570	-0.111
Perceived Ease of Use	4.412	0.485	-0.810	0.783
Trust in AI Chatbots	4.375	0.484	-1.284	2.826
Perceived Risk	4.428	0.475	-1.121	3.615
Human-Likeness	3.016	1.519	-0.054	-1.745
Prior Experience	4.483	0.491	-0.480	-0.645
Intention to Use	4.446	0.554	-0.930	1.073

Source: the table was compiled by the author using the research results.

3.5 Hypothesis testing

This section presents the empirical test of all hypotheses posited in this research is given according to conceptual research model. The research hypotheses were tested on the basis of quantitative statistical tests to assess the relationship between the independent, mediating, moderating and dependent variables. In particular, the regression analysis has been used to test the direct effects whereas the mediation analysis has been performed to test the indirect role of trust. To evaluate the conditional effect of human-likeness, prior experience and perceive risk, moderation analysis was used. Combined, these analyses are an evaluation of the intended theoretical relations and make it possible to validate the research model.

H1: Data privacy concerns negatively impact Trust in AI chatbots.

H2: Perceived Usefulness positively impacts Trust in AI chatbots.

H4: Perceived Ease of Use positively impacts Trust in AI chatbots.

To test Hypotheses H1, H2, and H4, a multiple regression analysis was conducted with Trust in AI Chatbots as the dependent variable and Data Privacy Concerns, Perceived Usefulness, and Perceived Ease of Use as independent variables. The results of the regression analysis are presented in Table 14 (Annex 5).

Table 14 Regression analysis of H1, H2 and H4.

	Unstandardized Coefficients		Standardized Coefficients Beta	t	Sig.	Collinearity Statistics	
	B	Std. Error				Tolerance	VIF
(Constant)	1.919	0.434		4.421	< .001		
Data Privacy Concerns	0.054	0.073	0.049	0.745	.457	0.905	1.105
Perceived Usefulness	0.263	0.074	0.232	3.538	< .001	0.915	1.093
Perceived Ease of Use	0.234	0.065	0.235	3.587	< .001	0.918	1.089

Source: the table was compiled by the author using the research results.

The results show that Perceived Usefulness has a positive and statistically significant effect on trust ($\beta = 0.232$, $t = 3.538$, $p < .001$), indicating that users who perceive AI chatbots as useful are more likely to trust them. Therefore, **H2 is supported**.

Similarly, Perceived Ease of Use demonstrates a positive and statistically significant relationship with trust ($\beta = 0.235$, $t = 3.587$, $p < .001$). This suggests that an intuitive and easy-to-use chatbot interface enhances users' confidence and trust in the technology. Consequently, **H4 is supported**.

In contrast, Data Privacy Concerns do not have a statistically significant effect on trust ($\beta = 0.049$, $t = 0.745$, $p = .457$). Although the relationship is positive, it is weak and does not reach statistical significance. Thus, the proposed negative relationship is not confirmed and **H1 is rejected**.

Collinearity diagnostics confirm that multicollinearity is not a concern, as all tolerance values exceed 0.90 and VIF values are well below the recommended threshold.

H7: Human-Likeness moderates the relationship between Data Privacy Concerns and Trust, such that higher human-likeness enhances the positive impact of transparent privacy handling on Trust.

H8: Prior Experience with similar technology usage moderates the relationship between Data Privacy Concerns and Trust, such that users with more experience perceive less privacy risk and greater Trust.

To test Hypotheses H7 and H8, moderation analyses were conducted using linear regression with mean-centered variables. The results are presented in Tables 15 & 16 (Annexes 6 & 7).

Table 15 Moderation effect of human-likeness on the relationship between data privacy concerns and trust in AI chatbots.

Predictor	Unstandardized β	Std. Error	Standardized β	t-value	p-value	LLCI	ULCI
(Constant)	4.365	0.033		130.633	< .001	4.299	4.431
Data Privacy Concerns	0.143	0.123	0.078	1.165	.245	-0.099	0.385
Human-Likeness	-0.418	0.257	-0.116	-1.626	.105	-0.924	0.088
Data Privacy Concerns x Human-Likeness	1.448	0.899	0.115	1.611	.109	-0.323	3.219

Source: the table was compiled by the author using the research results.

Table 16 Moderation effect of prior experience on the relationship between data privacy concerns and trust in AI chatbots.

Predictor	Unstandardized β	Std. Error	Standardized β	t-value	p-value	LLCI	ULCI
(Constant)	4.372	0.034		127.064	< .001	4.305	4.440
Data Privacy Concerns	0.121	0.126	0.066	0.965	.335	-0.127	0.369
Prior Experience	-0.161	0.191	-0.062	-0.846	.398	-0.537	0.215
Data Privacy Concerns x Prior Experience	0.892	0.640	0.103	1.394	.165	-0.369	2.153

Source: the table was compiled by the author using the research results.

The results indicate that the interaction between Data Privacy Concerns and Human-Likeness is not statistically significant (p = .109). This suggests that the degree of chatbot human-likeness does not significantly influence how data privacy concerns affect trust. Consequently, **H7 is rejected**.

Similarly, the interaction between Data Privacy Concerns and Prior Experience is not statistically significant (p = .165). This indicates that prior experience with similar technologies does not significantly alter the relationship between privacy concerns and trust. Therefore, **H8 is rejected**.

H3: Perceived Usefulness positively impacts the Intention to Use AI chatbots in online banking.
H5: Perceived Ease of Use positively impacts the Intention to Use AI chatbots in online banking.
H10: Trust in AI positively influences the Intention to Use AI chatbots in online banking among millennials.

To test Hypotheses H3, H5, and H10, a multiple regression analysis was conducted with Intention to Use AI Chatbots as the dependent variable and Perceived Usefulness, Perceived Ease of Use, and Trust in AI Chatbots as independent variables. The results are presented in Table 17 (Annex 8).

Table 17 Regression analysis of H3, H5 and H10.

	Unstandardized Coefficients		Standardized Coefficients Beta	t	Sig.	Collinearity Statistics	
	B	Std. Error				Tolerance	VIF
(Constant)	1.666	0.469		3.555	< .001		
Perceived Usefulness	0.302	0.086	0.233	3.508	< .001	0.896	1.116
Perceived Ease of Use	0.110	0.076	0.097	1.458	< .001	0.895	1.118
Trust in AI chatbots	0.215	0.078	0.188	2.772	.146	0.856	1.168

Source: the table was compiled by the author using the research results.

The results indicate that Perceived Usefulness has a positive and statistically significant effect on intention to use ($\beta = 0.233$, $t = 3.508$, $p < .001$). This confirms that users are more willing to adopt AI chatbots when they perceive them as beneficial and efficient. Therefore, **H3 is supported**.

However, Perceived Ease of Use does not show a statistically significant effect on intention to use ($\beta = 0.097$, $t = 1.458$, $p = .146$). This suggests that ease of use alone does not directly motivate behavioral intention when other factors are considered. Consequently, **H5 is rejected**.

Furthermore, Trust in AI Chatbots has a positive and statistically significant effect on intention to use (β = 0.188, t = 2.772, p = .006). This result indicates that trust plays a crucial role in translating positive perceptions into adoption intentions. Thus, **H10 is supported**.

Collinearity statistics again confirm that multicollinearity is not a concern, as VIF values remain close to 1 and tolerance levels are well above the acceptable minimum.

H9: Trust in AI chatbots mediates the relationship between Data Privacy Concerns and Intention to Use AI chatbots.

To test Hypothesis H9, a mediation analysis was conducted using JASP to examine whether Trust in AI Chatbots mediates the relationship between Data Privacy Concerns and Intention to Use AI Chatbots. The analysis was performed using maximum likelihood estimation with a 95% confidence interval, the results are presented in Table 18 (Annex 9).

Table 18 Mediation Analysis Results for Hypothesis H9.

Effect Type	Path	Std. Estimate (β)	Std. Error	z-value	p-value	95% Confidence Interval
Direct Effect	Data Privacy Concerns → Intention to Use	0.060	0.076	0.792	.428	[−0.094, 0.205]
Indirect Effect	Data Privacy Concerns → Trust → Intention to Use	0.044	0.022	2.032	.042	[0.012, 0.104]
Total Effect	Data Privacy Concerns → Intention to Use	0.105	0.076	1.384	.166	[−0.051, 0.248]
Path a	Data Privacy Concerns → Trust	0.161	0.076	2.123	.034	[0.012, 0.313]

Path b	Trust → Intention to Use	0.275	0.097	2.853	.004	[0.094, 0.469]

Note. Bootstrap confidence intervals based on 5,000 samples. Estimator = Maximum Likelihood (ML). *Source: the table was compiled by the author using the research results.*

The results indicate that Data Privacy Concerns have a significant positive effect on Trust in AI Chatbots (β = 0.161, z = 2.123, p = .034), demonstrating that users' perceptions regarding data privacy are significantly associated with their level of trust in AI chatbots. Furthermore, Trust in AI Chatbots has a significant positive effect on Intention to Use (β = 0.275, z = 2.853, p = .004), indicating that higher levels of trust increase users' willingness to adopt AI chatbot services.

The indirect effect of Data Privacy Concerns on Intention to Use through Trust was found to be statistically significant (β = 0.044, z = 2.032, p = .042), with a 95% confidence interval that does not include zero (CI = [0.012, 0.104]). This confirms the presence of a mediation effect.

In contrast, the direct effect of Data Privacy Concerns on Intention to Use was not statistically significant (β = 0.060, z = 0.792, p = .428), and the total effect was also non-significant (β = 0.105, z = 1.384, p = .166). These findings indicate that Data Privacy Concerns do not directly influence users' intention to use AI chatbots; instead, their effect is transmitted entirely through Trust in AI Chatbots.

Taken together, the results demonstrate that Trust fully mediates the relationship between Data Privacy Concerns and Intention to Use AI chatbots. Therefore, **H9 is supported**.

H6: Perceived Risk moderates the relationship between Trust in AI chatbots and Intention to Use, such that the positive effect of Trust is weaker under high perceived risk.

To test Hypothesis H6, a moderation analysis was conducted using linear regression. Trust and perceived risk were mean centered prior to computing the interaction term in order to reduce multicollinearity and facilitate interpretation. Intention to use AI chatbots was specified as the dependent variable, while centered trust, centered perceived risk, and their interaction term were entered as predictors, the results are presented in Table 19 (Annex 10).

Table 19 Moderating effect of perceived risk on the relationship between trust in AI chatbots and intention to use.

Predictor	**Unstandardized β**	**Std. Error**	**Standardized β**	**t-value**	**p-value**	LLCI	ULCI
(Constant)	4.372	0.034		127.064	< .001	4.305	4.440
Trust	0.233	0.129	0.125	1.807	.072	-0.127	0.369
Perceived Risk	0.646	0.290	0.148	2.230	.027	-0.537	0.215
Trust x Perceived Risk	−1.406	0.975	−0.100	−1.442	.151	-0.369	2.153

Source: the table was compiled by the author using the research results.

The overall regression model was statistically significant ($R^2 = 0.041$, $F(3, 217) = 3.129$, $p = .027$), indicating that the predictors jointly explain approximately 4.1% of the variance in intention to use AI chatbots.

The results show that perceived risk has a significant positive direct effect on intention to use ($\beta = 0.148$, $p = .027$). Trust, however, does not have a statistically significant direct effect on intention to use when perceived risk and the interaction term are included in the model ($\beta = 0.125$, $p = .072$).

Crucially, the interaction term between trust and perceived risk is not statistically significant ($\beta = -0.100$, $p = .151$). This indicates that perceived risk does not significantly alter the strength or direction of the relationship between trust in AI chatbots and intention to use.

Therefore, although perceived risk independently influences intention to use, it **does** not function as a moderator in the relationship between trust and intention to use AI chatbots. Consequently, **H6 is rejected**.

In conclusion, the hypothesis testing results provide partial support for the proposed research model. The findings confirm that perceived usefulness and perceived ease of use are significant antecedents of trust, while trust itself plays a central role in driving intention to use AI

chatbots in online banking. Perceived usefulness also directly influences intention to use. In contrast, data privacy concerns do not directly reduce trust, and several proposed moderating effects were not supported.

Overall, the results highlight trust as a key mechanism through which perceptions related to usefulness and privacy translate into behavioral intention. These findings form a strong empirical basis for the discussion of results presented in the following chapter.

Table 20 Summary of hypothesis testing results.

Hypothesis	Result
H1: Data privacy concerns negatively impact Trust in AI chatbots.	Rejected
H2: Perceived Usefulness positively impacts Trust in AI chatbots.	Supported
H3: Perceived Usefulness positively impacts the Intention to Use AI chatbots in online banking.	Supported
H4: Perceived Ease of Use positively impacts Trust in AI chatbots.	Supported
H5: Perceived Ease of Use positively impacts the Intention to Use AI chatbots in online banking.	Rejected
H6: Perceived Risk moderates the relationship between Trust in AI chatbots and Intention to Use, such that the positive effect of Trust is weaker under high perceived risk.	Rejected
H7: Human-Likeness moderates the relationship between Data Privacy Concerns and Trust, such that higher human-likeness enhances the positive impact of transparent privacy handling on Trust.	Rejected
H8: Prior Experience with similar technology usage moderates the relationship between Data Privacy Concerns and Trust, such that users with more experience perceive less privacy risk and greater Trust.	Rejected
H9: Trust in AI chatbots mediates the relationship between Data Privacy Concerns and Intention to Use AI chatbots.	Supported
H10: Trust in AI positively influences the Intention to Use AI chatbots in online banking among millennials.	Supported

Source: the table was compiled by the author using the research results.

3.6 Discussion of results

This section provides a discussion of the empirical results has been found by referring them to the theoretical framework and the previous studies. The discussion is presented

according to the framework of the research model and hypotheses, which are the formation of trust, intention to use AI chatbots in online banking, and the functions of moderating and mediating variables. Results interpretation is consistent with Technology Acceptance Model, Trust Theory and Privacy Calculus Theory as they were discussed in Chapter 2.

3.6.1 Antecedents of Trust in AI Chatbots

The findings suggest that Perceived Usefulness and Perceived Ease of Use have a strong predictive effect on trust in AI chatbots, whereas Data Privacy Concerns have no direct significant effect on trust.

The assumptions of the Technology Acceptance Model are supported by the positive influence of the perceived usefulness on trust, which implies that the users should form positive attitudes and develop trust in technologies that can facilitate the performance of the tasks. When applied to online banking, AI chatbots that are viewed as effective and useful make users more confident in the technology. The finding aligns with all other studies that perceived usefulness is a main determinant of trust towards digital financial services (Davis, 1989; Venkatesh and Davis, 2000; Giordani and Ferreira, 2023).

Likewise, perceived ease of use was also found to affect trust positively. This result indicates that consumers have less cognitive load and doubt with the intervention of AI chat bots being viewed as user-friendly and intuitive, which consequently enhances emotional reassurance and fosters trust. This finding is consistent with the existing literature on the topic that proved usability to decrease the perceived complexity and increase trust, especially in technology mediated service experience (Gefen et al., 2003; Venkatesh and Bala, 2008; Lappeman et al., 2022).

On the other hand, there was no statistically significant impact on trust in AI chatbots on the data privacy concerns. This observation is contrary to the previous research which has found privacy concerns to be a significant impediment to online technology trust (Dinev and Hart, 2006; Malhotra et al., 2004; Beldad et al., 2011). One of the potential reasons is that respondents might take it as a matter of basal level of data protection in regulated banking settings and consider the issues of privacy level less important. Moreover, due to an understanding of the digital services provided and the daily exposure of millennials to the share of online information, the direct impact of the issue of privacy on trust might be reduced, especially in the case of hypothetical or scenario-based communication between people and chatbots (Lappeman et al., 2022; Pelote, 2022).

3.6.2 Determinants of Intention to Use AI Chatbots

The findings indicate that the Perceived Usefulness and Trust in AI Chatbots can have a positive impact on Intention to Use significantly, but Perceived Ease of Use does not have a direct impact on Intention to Use in the presence of other variables.

The great influence of the perceived usefulness on intention to use supports its leading position in the Technology Acceptance Model. Users will be more inclined to use AI chatbots when they consider the technology to have a real-value contribution, including faster service, convenience, and better resolution of a problem. This observation is in line with other studies on the adoption of technologies in online banking and AI-based services (Davis, 1989; Venkatesh & Davis, 2000; Alalwan et al., 2017; Lappeman et al., 2022).

It was also determined that trust was also a strong predictor of the intention to use, pointing out its critical importance in high-risk situations like financial services. Users who feel that AI chatbots are trustful, safe and are in their best interest are more inclined to use the technology. This finding confirms Trust Theory and validates previous empirical results that trust is an important mechanism that can convert positive perceptions into behavioral intention.

Interestingly, intention to use was not significantly directly influenced by perceived ease of use. This implies that to digitally experienced users, such as millennials, ease of use can be viewed as a simple necessity and not one that can decisively affect the adoption process. This observation is consistent with the existing studies which indicate that the context of ease-of-use decreases over time as the user gets familiar to the technology (Venkatesh et al., 2003; Venkatesh & Bala, 2008; Alalwan et al., 2017).

3.6.3 The Role of Perceived Risk, Human-Likeness, and Prior Experience

As the analysis reveals several of the suggested moderating effects were not supported. There was no significant interaction between perceived risk and the relationship between trust and intention to use or human-likeness and prior experience and the relationship between data privacy concerns and trust.

The moderate effect of perceived risk is not significant, indicating that risk perception might have a direct impact on intention to use but the degree of influence is not significant to change the existence of the trust-intention relationship. This could imply that trust is a constant

determinant of intention irrespective of different perceived risk in the environment of online banking chatbots.

Another similarity between the two studies is the non-moderating role of human-likeness and previous experience, which means that the issue of privacy on the basis of trust cannot be simplified by the design of chatbots or the familiarity of the user with AI-based solutions. Users can assess the risk of data privacy without any prior experience to talk with similar technology and regardless of the conversational style used. These results go in opposition to certain studies of human-computer interaction (Epley & Waytz, 2010; Sheehan et al., 2020) but agree with studies that illustrated that privacy concerns are strongly context-dependent and less sensitive to interface design features (Dinev & Hart, 2006; Malhotra et al., 2004; Beldad et al., 2011).

3.6.4 Mediating Role of Trust

The mediation analysis shows that Trust completes the relationship between Data Privacy Concerns and Intention to Use AI Chatbots. This observation confirms Privacy Calculus Theory, which states that users balance the perceived risks and the perceived benefits in making a decision about adopting a technology.

These findings show that data privacy concerns do not have a direct impact on intention to use but rather indirectly by trust. Trust is destroyed when privacy issues are compromised, and this reduces the willingness of users to use AI chatbots. On the other hand, privacy concerns have less effect on behavioral intention in the case of establishment of trust. This emphasizes on trust as a key process by which perceptions of privacy influence the adoption decisions.

In summary, the results prove the presence of perceived usefulness and perceived ease of use as the main antecedents of trust in AI chatbots, and the direct relationship between trust and perceived usefulness with intention to use in online banking. Trust was also a key mediating variable between the concern of data privacy and intention to use, with some of the hypothesized moderating effects rejected.

Overall, the findings highlight the value of creating trustful, helpful, and convenient AI chatbot applications in the financial industry. Such observations form a good basis on the conclusions and practical implications adopted in the next chapter.

CONCLUSIONS AND RECOMMENDATIONS

The aim of this research was to investigate the effects of the data privacy concerns and the impact it had on trust and intention to use AI chatbots in online banking websites among millennials. To this end, the study integrated three clearly proven theoretical frameworks, Technology Acceptance Model (TAM), Trust Theory and Privacy Calculus Theory, and examined their suitability in the framework of AI-based financial services.

Theoretically, the research proves that the adoption of technology in high-risk service settings like in online banking cannot be attributed to elements of functionality only. Although perceived usefulness and perceived ease of use are also significant, trust has become one of the key mechanisms through which the perceptions of users are converted to behavioral intention. The implementation of the trust and data privacy concerns into TAM not only expands the existing knowledge on technology acceptance but also proves the usefulness of the functional, psychological, and ethical aspects in order to investigate AI adoption.

The empirical results show that the perceived usefulness and the perceived ease of use are important antecedents of trust in AI chatbots. Once millennials start finding chatbots useful, efficient, and easy to deal with, they will gain confidence in the technology. This confirms that TAM can be used in the area of AI chatbots and emphasize the role of trust as a necessary addition of the model in the financial industry.

The findings also indicate that trust and perceived usefulness are the two key factors behind intention to use AI chatbots. In online banking where there is a high level of uncertainty and perceived risk, trust is very crucial. Although users may realize the practical use of AI chatbots, their readiness to use the technology will largely depend on their trust in the chatbot system and the institution itself.

Quite on the contrary, there was no direct negative impact of data privacy concerns on trust and no direct positive impact of perceived ease of use on intention to use. These results indicate that in the case of digitally experienced users, including millennials, privacy protection and usability can be viewed not as factors leading to adoption decision but some minimum condition. Nevertheless, the importance of privacy concerns is indirect since their mediating importance on intention to use is completely mediated by trust.

The mediation analysis proves that trust is the key mediator between the issue of data privacy and the intention to use AI chatbots. This result empirically validates Privacy Calculus Theory in the sense that millennials think many judgments about privacy threats in terms of trust as opposed to actual behavior.

Besides, perceived risk, human-likeness, or prior experience did not produce any significant moderating effect in the study. This indicates that the trust-building process is similar at various levels of perceived risk, chatbot design characteristics and familiarity of the users with the online banking. These findings suggest that institutional guarantees and perceived system reliability can be stronger factors of trust development than user characteristics or design features.

In general, the study is relevant to the scholarly literature because it offers a comprehensive framework that justifies the adoption of AI chatbots by the interplay of technology acceptance, trust, and privacy factors. On a methodological level, it illustrates the usefulness of the mediation and moderation analysis in discovering the multifaceted relationships in the study of AI adoption. In practice, it provides the understanding of how the banks can build trust and promote responsible use of AI chatbots among millennial users.

Practical Recommendations for Banks and Financial Service Providers

Based on the conclusions made in this paper, it is possible to offer several suggestions to banks and other financial institutions that adopt AI chatbots:

1. Enhance Functional Usefulness

Banks ought to focus on the practical value of AI chatbots by making sure that they are rapid, precise, and significant. True-time transaction support, management of accounts and solutions of a problem should be highlighted to further bolster perceived usefulness which has direct impact on trust and intention to use.

2. Design for Simplicity and Trust Building

Even though the intention to use does not have a direct relationship with perceived ease of use, it plays a significant role in trust. To support adoption indirectly by enhancing trust, banks

should invest in a friendly chatbot interface, well-defined conversational flows, and error-free interactions.

3. Strengthen Transparency and Communication

The way chatbots work, the types of data they gather, and the safety of customer information should be well explained to the financial institutions by the financial institutions. The clarity of chatbot capabilities, limitations, and security measures may decrease uncertainty and act as a source of institutional trust.

4. Implement and Signal Strong Data Protection Practices

Because trust is the bridging factor between the data privacy concerns and the intention to use, banks must not just act in accordance with the rules of data protection but also inform people of it. Public privacy policies, authentications, and guarantees regarding data utilization would go a long way in improving the perceptions of trust.

Recommendations for the Scientific Community and Future Research

In addition to practical implications, this study offers several directions for future academic research:

1. Extend the Model to Other User Groups and Contexts

Further research could use the suggested combined model with other generational groups or other industries to determine whether the role of trust and privacy varies in different situations.

2. Incorporate Longitudinal Research Designs

This research is intended to be used at one point. Longitudinal designs maybe used to investigate the change in the levels of trust and privacy with repeated chatbot use.

3. Explore Additional Psychological and Ethical Variables

Future studies can look at the inclusion of constructs like perceived transparency, AI explainability, or algorithmic fairness to bring additional insights on AI adoption in sensitive areas.

4. Compare Human-Like vs. Functional Chatbot Designs Experimentally

Human-likeness did not moderate relationships in this paper; however, controlled experimental designs could offer greater information on the effect of various chatbot personalities on trust and privacy perceptions.

In conclusion, this study has shown that the level of uptake of AI chatbots in online banking by millennials is mainly due to trust and perceived usefulness and not privacy concerns and ease of use, exclusively. Trust is a very central mechanism that aids in converting the perception of privacy into behavioral intention. The combination of the TAM, Trust Theory, and Privacy Calculus Theory provides a more profound insight into how the functional advantages, psychological certainty, and moral principles are intertwined to influence the use of AI chatbots. These lessons can be important both to scholars interested in the further development of the theory and to practitioners who are willing to develop credible and user-oriented AI-based solutions in the financial services industry.

LIMITATIONS AND DIRECTIONS FOR FUTURE RESEARCH

Regardless of its contributions, this study has several limitations that can be recognized.

1. The research was based on self-reported information and hypothetical situations of chatbot use, which might be insufficient to reflect the behavior of the user. The findings can be validated by using experimental design or actual usage information in the future.
2. The sample was mainly concentrated on millennials, and thus the findings cannot be generalized to other age groups. Further studies may include the analysis of the generational differences in the adoption of AI chatbots in online banking.
3. This research paper has looked at the AI chatbots in a general online banking experience. Further studies might focus on particular features of chatbots or evaluate AI chatbots in dissimilar financial institutions or service settings.
4. Further research may introduce other psychological or contextual factors, including trust propensity, perceived transparency, or cultural factors, to further enhance the knowledge of the adoption of AI chatbots.

LIST OF FIGURES

LIST OF TABLES

REFERENCES

1. *Ahamed, A. F. M., Sandu, M. C., & Durst, S. (2024). Exploring online banking adoption intention among Millennials and Generation Z: A qualitative comparative analysis. Unpublished working paper.*
2. *Alagarsamy, S., & Mehrolia, S. (2023). Exploring chatbot trust: Antecedents and behavioural outcomes. Heliyon, 9(5).*
3. *Bhattacharya, C., & Sinha, M. (2022). The role of artificial intelligence in banking for leveraging customer experience. Australasian Accounting, Business and Finance Journal, 16(5). https://doi.org/10.14453/aabfj.v16i5.07*
4. *Bouhia, M., Rajaobelina, L., PromTep, S., Arcand, M., & Ricard, L. (2022). Drivers of privacy concerns when interacting with a chatbot in a customer service encounter. International Journal of Bank Marketing, 40(6), 1159–1181.*
5. *Cheng, Y., & Jiang, H. (2020). How do AI-driven chatbots impact user experience? Examining gratifications, perceived privacy risk, satisfaction, loyalty, and continued use. Journal of Broadcasting & Electronic Media, 64(4), 592-614. https://doi.org/10.1080/08838151.2020.1834296*
6. *Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. Organization Science, 10(1), 104–115.*
7. *De Cicco, R., Silva, S. C., & Alparone, F. R. (2020). Millennials' attitude toward chatbots: An experimental study in a social relationship perspective. International Journal of Retail & Distribution Management, 48(11), 1213–1233.*
8. *Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340.*
9. *Elkhatibi, Y., Guelzim, H., & Benabdelouahed, R. (2025). In-depth exploration of the factors influencing trust in chatbot integration: An exhaustive investigation within the banking sector. International Journal of Electronic Commerce Studies, 16(1).*
10. *Giordani, J. (2024). Mitigating chatbots AI data privacy violations in the banking sector: A qualitative grounded theory study. European Journal of Applied Science, Engineering and Technology, 2(4), 14-65.*
11. *Giordani, R. (2024). Data privacy breaches and consumer trust in AI-powered banking services. Journal of Financial Technology Studies, 9(1), 45–63.*

12. *Giordani, G., & Ferreira, A. (2023). Trust, transparency, and privacy in AI-driven financial chatbots: The moderating role of user experience. Computers in Human Behavior, 144, 107728.*
13. *Hasal, M., Tcherni, M., & Basar, A. (2021). The effect of privacy concerns on trust and adoption of digital banking services. Journal of Retailing and Consumer Services, 62, 102619.*
14. *Hasan, S., Godhuli, E. R., Rahman, M. S., & Al Mamun, M. A. (2023). The adoption of conversational assistants in the banking industry: is the perceived risk a moderator? Heliyon, 9(9). https://doi.org/10.1016/j.heliyon.2023.e20220*
15. *Hasal, M., Nowaková, J., Saghair, K. A., Abdulla, H., & Snášel, V. (2021). Chatbots: Security, privacy, data protection, and social aspects. Concurrency and Computation: Practice and Experience, 33(19), e6426.*
16. *Kelly, S., Kaye, S. A., & Oviedo-Trespalacios, O. (2022). A multi-industry analysis of the future use of AI Chatbots. Human Behavior and Emerging Technologies, 2022(1), 2552099. https://doi.org/10.1155/2022/2552099*
17. *Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2022). Trust and digital privacy: willingness to disclose personal information to banking chatbot services. Journal of Financial Services Marketing, 28(2), 337. https://doi.org/10.1057/s41264-022-00154-z*
18. *Limakrisna, N., & Moeins, A. (2024). Intelligent banking chatbot: Intention to continue through millennial customer satisfaction in Indonesia using the TAM method. Dinasti International Journal of Economics, Finance & Accounting, 4(6).*
19. *Lubbe, I., Roberts-Lombard, M., & Langerman, J. (2025). Millennials' experiences and satisfaction with chatbots: A study of self-service technology in emerging markets. European Business Review, 37(4), 741–769.*
20. *Luo, C., Li, Y., Zhang, J., & Shim, J. P. (2021). Examining multi-dimensional trust and privacy in the adoption of AI chatbots for banking services. Information Systems Frontiers, 23(6), 1549–1565. https://doi.org/10.14329/apjis.2023.33.3.652*
21. Lappeman, J., Marlie, S., Johnson, T., & Poggenpoel, S. (2022). Trust and digital privacy: Willingness to disclose personal information to banking chatbot services. *Journal of Financial Services Marketing*, *28*(2), 337–357. *https://doi.org/10.1057/s41264-022-00154-z*
22. Lubbe, I., Roberts-Lombard, M., & Langerman, J. (2025). Millennials' experiences and satisfaction with chatbots: A study of self-service technology in emerging markets. *European Business Review*, *37*(4), 741–769. *https://doi.org/10.1108/EBR-06-2024-0190*

23. *Lappeman, J., Egan, P., & Egan, T. (2022). Chatbots, AI, and the digital banking customer experience: Understanding trust and perceived usefulness in financial services. Journal of Financial Services Marketing, 27(2), 97–110.*
24. Lubbe, D., Du Plessis, C., & Botha, E. (2023). Building trust in conversational AI: Privacy, transparency, and user confidence in financial chatbots. *Journal of Retailing and Consumer Services, 75*, 103428.
25. *Mucsková, M. (2024). Transforming banking with artificial intelligence: Applications, challenges, and implications. Trends Economics and Management, 18(42), 21-37.*
26. *Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709–734.*
27. *Mehrolia, S., Alagarsamy, S., Moorthy, V., & Jeevananda, S. (2023). Will users continue using banking chatbots? The moderating role of perceived risk. FIIB Business Review.*
28. *McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334–359.*
29. *Ngu Ngendi, H. P. (2024). The Influence of AI on Millennial Consumer Behavior: online shopping in Finland.*
30. *Ngu Ngendi, T. (2024). Privacy, trust and user intentions: Examining AI chatbot adoption in digital banking. Journal of Financial Technology and Innovation, 12(3), 45–63.*
31. *Ng, M., Coopamootoo, K. P., Toreini, E., Aitken, M., Elliot, K., & van Moorsel, A. (2020, September). Simulating the effects of social presence on trust, privacy concerns, and usage intentions in automated bots for finance. In 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 190–199). https://doi.org/10.1109/EuroSPW51379.2020.00034*
32. Patil, K., & Kulkarni, M. S. (2019). Artificial intelligence in financial services: Customer chatbot advisor adoption. *International Journal of Innovative Technology and Exploring Engineering*, *9*(1), 4296–4303.
33. *Pelote, M. L. dos S. M. (2022). Being at the cutting edge of internet banking: The role of privacy perception and the consumer determinants of intention to adopt AI technologies. Master's Thesis, Universidade NOVA de Lisboa (Portugal).*
34. *Rohit, K., Kumari, P., Singh, N., & Alofaysan, H. (2025). Smart banking chatbots and consumer engagement: The role of trust and privacy in AI-driven banking. Journal of Strategic Marketing, 1–18.*

35. *Rahman, M., Ming, T. H., Baigh, T. A., & Sarker, M. (2023). Adoption of artificial intelligence in banking services: An empirical analysis. International Journal of Emerging Markets, 18(10), 4270–4300. https://doi.org/10.1108/IJOEM-06-2020-0724*
36. Rohit, K., Kumari, P., Singh, N., & Alofaysan, H. (2025). Smart banking chatbots and consumer engagement: The role of trust and privacy in AI-driven banking. *Journal of Strategic Marketing*. Advance online publication. *https://doi.org/10.1080/0965254X.2025.2481140*
37. Sfar, N., Sboui, M., & Baati, O. (2025). The impact of chatbot anthropomorphism on customer experience and chatbot usage intention: A technology acceptance approach. *International Journal of Quality and Service Sciences*, *17*(2), 168–194.
38. *Suhartanto, D., Syarief, M. E., Chandra Nugraha, A., Suhaeni, T., Masthura, A., & Amin, H. (2022). Millennial loyalty towards artificial intelligence-enabled mobile banking: evidence from Indonesian Islamic banks. Journal of Islamic Marketing, 13(9), 1958-1972. https://www.emerald.com/insight/1759-0833.htm*
39. *Shaikh, I. A. K., Khan, S., & Faisal, S. (2023). Determinants affecting customer intention to use chatbots in the banking sector. Innovative Marketing, 19(4), 257-268. http://dx.doi.org/10.21511/im.19(4).2023.21*
40. *Saxena, C., Kumar, P., Sarvaiya, R., & Khatri, B. (2023, May). Attitude, behavioral intention and adoption of AI driven chatbots in the banking sector. In 2023 IEEE IAS global conference on emerging technologies (GlobConET) (pp. 1-8). IEEE.*
41. *Satheesh, M., & Nagaraj, S. (2021). Applications of artificial intelligence on customer experience and service quality of the banking sector. International Management Review, 17(1), 9–86.*
42. *Sfar, N., Sboui, M., & Baati, O. (2025). The impact of chatbot anthropomorphism on customer experience and chatbot usage intention: A technology acceptance approach. International Journal of Quality and Service Sciences, 17(2), 168–194.*
43. *Saunders, M., Lewis, P., & Thornhill, A. (2019). Research methods for business students (8th ed.). Pearson Education Limited.*
44. *Skewness & kurtosis definition and use. https://www.geeksforgeeks.org/data-science/difference-between-skewness-and-kurtosis/*
45. *Thanh, N. P. Q., & Linh, C. D. (2024). Factors affecting the decision to use chatbots in e-banking services of GenZ customers in Vietnam. Journal of Infrastructure, Policy and Development, 8(13), 9688. https://doi.org/10.24294/jipd9688*
46. Toreini, E., Aitken, M., Coopamootoo, K., Elliott, K., Zelaya, C. G., & van Moorsel, A. (2020). The relationship between trust in AI and trustworthy machine learning technologies. In

*Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency (FAT '*20)* (pp. 272–283). Association for Computing Machinery. *https://doi.org/10.1145/3351095.3372834*

47. *Toh, T. J., & Tay, L. Y. (2022). Banking chatbots: A study on technology acceptance among millennials in Malaysia. Journal of Logistics, Informatics and Service Science, 9(3), 1–15.*
48. *Uddin, M. N., Thiam Low, W., Afjalur Rahman, M., & Mokhtar, S. (2024, May). An Exploration of Millennials' Attitudes Towards the Use of Artificial Intelligence Chatbots for Customer Service within E-commerce Platforms. In Proceedings of the International Conference on Business, Management and Leadership (Vol. 1, No. 1, pp. 1-19). https://doi.org/10.33422/icbml.v1i1.374*
49. *Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies.* Management Science, 46*(2), 186–204.*
50. *Wube, H. D., Esubalew, S. Z., Weldesellasie, F. F., & Debelee, T. G. (2022). Text-based chatbot in financial sector: A systematic literature review. Data Science in Finance and Economics, 2(3), 232–259.*
51. *Yussaivia, A. M., Lub, C. Y., Syarief, M. E., & Suhartanto, D. (2021). Millennial experience with mobile banking and AI-enabled mobile banking: Evidence from Islamic banking. International Journal of Applied, 3(1), 39–53.*

ANNEXES

Annex 1

Dear participant,
You are invited to take part in a research study titled *"The Influence of Data Privacy Concerns on Trust and Intention to Use AI Chatbots in Online Banking Platforms: The Case of Millennials."*

The purpose of this study is to understand how millennials perceive and use AI chatbots in online banking, particularly how data privacy, trust, and technology perceptions influence their behavioral intentions.

Participation is **voluntary** and **anonymous**. The survey will take approximately 7–10 minutes. Your responses will be used **only for academic research purposes** and handled in compliance with **GDPR (2018)** standards.

By clicking "Next," you confirm that you have read this information and voluntarily agree to participate.

1. Age Eligibility

Please select the age group to which you belong:

- ☐ 29–34 years
- ☐ 35–40 years
- ☐ I do not fall within this age range

If the participant selects "I do not fall within this age range" display this message:
Thank you for your interest. Unfortunately, you are not part of the target demographic for this study.

2. Online Banking Usage Frequency

How often do you use online banking services (app or website)?

- ☐ Daily

- ☐ Several times per week
- ☐ Once per week
- ☐ Several times per month
- ☐ Rarely → *Terminate survey automatically (not a suitable digital user)*

Termination message:
Thank you for your interest. This study focuses on regular online banking users.

3. Previous Experience with Banking Chatbots

Have you used an AI chatbot provided by an online banking platform within the last 12 months?

- ☐ Yes, I have used a banking chatbot before → *Terminate survey*
- ☐ No, I have never used a banking chatbot → *Continue*

Termination message:
Thank you for your interest. This study focuses on first-time users only.

4. Experience With Other AI Technologies

Have you used other AI-based digital assistants (e.g., Siri, Alexa, ChatGPT, Google Assistant, e-commerce chatbots) in the last 6 months?

- ☐ Yes
- ☐ No

Instructions for answering the following questions:
In the next sections, you will be asked to evaluate different statements related to your perceptions of AI chatbots in online banking.

Please indicate how much you agree or disagree with each statement based on the hypothetical scenario provided to you.

The evaluation scale is as follows:
1 – Strongly Disagree

2 – Disagree

3 – Neutral

4 – Agree

5 – Strongly Agree

There are no right or wrong answers. Please respond honestly based on your own feelings and expectations.

Hypothetical Chatbot Scenario

Imagine that your bank introduces a new AI chatbot that would help customers handle basic banking tasks (balance checks, transfers, information requests). Based on this hypothetical situation, please indicate how you would feel about the following statements.

Data Privacy Concerns (DPC)

The following items measure your concerns regarding security, transparency, and fairness in how the chatbot may handle your data.

A. Data Security Concerns (DPC-S)

Risk of breaches, unauthorized access; adapted from Dinev & Hart (2006); Malhotra et al. (2004)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I would be concerned that my chatbot interactions might not be securely protected.					
I would worry that unauthorized parties could access my banking information.					
I would be concerned about possible data breaches involving the chatbot.					

B. Data Transparency Concerns (DPC-T)

Lack of clarity about data use; adapted from Bellman et al. (2004); Beldad et al. (2011)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I would feel uncomfortable if the bank did not clearly explain how chatbot data are used.					
I would feel there is not enough transparency about how the chatbot handles my data.					
I would worry if the chatbot did not clearly state what information it collects from me.					

C. Data Fairness Concerns (DPC-F)

Misuse, unnecessary collection; adapted from Smith et al. (1996); Martin (2019)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I would be concerned that the chatbot could use my data in ways I did not.					
I would feel the chatbot might collect more information than is necessary.					
I would worry that my data could be used for purposes not directly related to banking.					

Perceived Usefulness (PU)

This section measures how useful the banking chatbot would be for managing your banking activities. (Source: Davis, 1989; Venkatesh & Davis, 2000)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Using the bank's chatbot would make managing my banking tasks more efficient.					
The chatbot would improve the quality of my banking service experience.					
Using the chatbot could save me time compared to visiting a bank branch.					
Overall, I would find the chatbot useful for completing my banking activities.					

Perceived Ease of Use (PEOU)

This section measures how easy the chatbot would be to learn and operate. (Source: Davis, 1989; Venkatesh & Bala, 2008)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
Interacting with the chatbot would be clear and understandable.					
Learning to use the chatbot would be easy for me.					

The chatbot would be easy to navigate.					
Overall, I would find the chatbot simple would be to use.					

Trust in AI Chatbots (TR)

In this section, please evaluate your trust in AI chatbots. (Source: McKnight et al., 2002; Lappeman et al., 2022)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I would trust the chatbot to provide accurate information.					
I would believe the chatbot handles my data responsibly.					
I would trust the chatbot to act in my best interest.					
The chatbot would behaves reliably when I use it.					
Overall, I would have confidence in the chatbot system.					

Perceived Risk (PR)

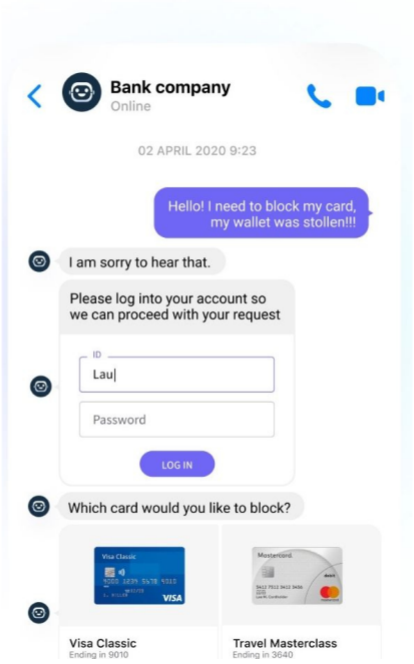
This section examines your concerns about potential risks associated with using an AI banking chatbot. (Source: Featherman & Pavlou, 2003; Beldad et al., 2011)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I feel that using the chatbot might expose my personal data to risks.					
There is a chance that my banking information could be misused through the chatbot.					
I think there are security risks when using AI chatbots for banking.					
I am concerned that my privacy could be violated when using the chatbot.					

Human-Likeness (HL)

Scenario A: Highly human-like chatbot

Imagine that your bank introduces a new AI chatbot. Below you will see a short example of how a banking AI chatbot could communicate.



Source: the picture was taken from google image and modified by the author.

Based on this example, please evaluate the statements below.

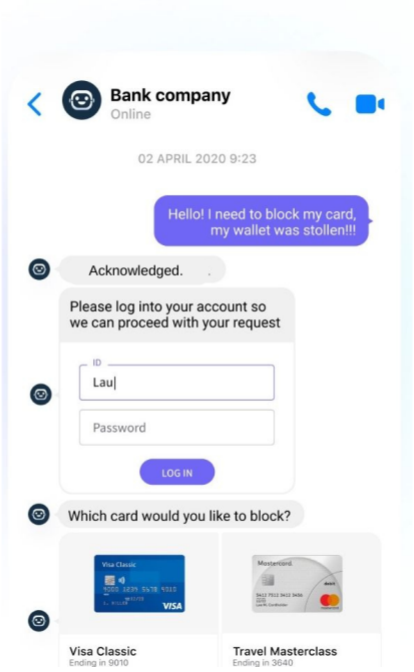
Scale: 1 = Strongly Disagree → 5 = Strongly Agree

(Source: Epley & Waytz, 2010; Sheehan et al., 2020)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The chatbot communicates in a human-like manner.					
The chatbot's tone feels natural and conversational.					
I feel that the chatbot understands my needs like a human representative.					
The chatbot's personality makes the interaction more engaging.					

Scenario B: Robotic, machine-like chatbot

Imagine that your bank introduces a new AI chatbot. Below you will see a short example of how a banking AI chatbot could communicate.



Source: the picture was taken from google image and modified by the author.

Based on this example, please evaluate the statements below.

Scale: 1 = Strongly Disagree → 5 = Strongly Agree

(Source: Epley & Waytz, 2010; Sheehan et al., 2020)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
The chatbot communicates in a human-like manner.					
The chatbot's tone feels natural and conversational.					
I feel that the chatbot understands my needs like a human representative.					

The chatbot's personality makes the interaction more engaging.					

Part 9: Prior Experience (PE)

This section asks about your familiarity with other AI systems and digital technologies. (Source: Gefen et al., 2003)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I have experience using other AI-based systems or chatbots.					
I frequently use digital technologies for banking or financial management.					
I feel confident using AI tools in online environments.					

Part 10: Intention to Use (IU)

This section measures your future intention to use the banking chatbot. (Source: Venkatesh & Davis, 2000; Lappeman et al., 2022)

Item	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I plan to try the chatbot in banking in the near future to see how it works.					

I am likely to use the chatbot regularly for banking tasks.					
I intend to continue using the bank's chatbot in the future.					

Part 11: Demographic Information

Please provide the following background information. Your answers will remain anonymous and will be used only for statistical purposes.

1. Gender:

Please indicate your gender:

☐ Male ☐ Female ☐ Other / Prefer not to say

2. Country:

Please indicate your current country of residence:

……

3. Education level

Please indicate your highest completed level of education:

☐ High school ☐ Bachelor's ☐ Master's ☐ Doctorate ☐ Other

4. Employment status

Please indicate your current employment status:

☐ Student ☐ Employed ☐ Self-employed ☐ Unemployed

5. Income level:

Please indicate your approximate monthly income:

☐ Less than €1,000 ☐ €1,000–€1,999 ☐ €2,000–€2,999 ☐ €3,000 or more ☐ Prefer not to say

Closing Message

Thank you for taking the time to participate in this study. Your responses are valuable and will contribute to understanding how millennials perceive data privacy and trust when using AI chatbots in online banking.

Annex 2

- **Data Privacy Concerns**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.900			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

- **Perceive usefulness**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.762			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

- **Perceive ease of use**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.824			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

- **Trust in AI chatbots**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.811			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

- **Perceive risk**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.796			

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

- **Human-likeness**
    - **Human-likeness A**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.693			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

    - **Human-likeness B**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.797			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

- **Prior experience**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.816			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

- **Intention to use AI chatbots**

Frequentist Scale Reliability Statistics

			95% CI	
Coefficient	Estimate	Std. Error	Lower	Upper
Coefficient α	0.864			

Note. The analytic confidence interval is not available for coefficient alpha/lambda2 when data contain missings and pairwise complete observations are used. Try changing to 'Delete listwise' within 'Advanced Options'.

Source: the table was compiled by author using the software JASP.

Annex 3 & 4

Descriptive Statistics

	Mean	Std. Deviation	Skewness	Std. Error of Skewness	Kurtosis	Std. Error of Kurtosis	Shapiro-Wilk	P-value of Shapiro-Wilk
DSP_Total_mean	4.472	0.440	-0.998	0.164	1.612	0.326	0.907	< .001

Descriptive Statistics

	Mean	Std. Deviation	Skewness	Std. Error of Skewness	Kurtosis	Std. Error of Kurtosis	Shapiro-Wilk	P-value of Shapiro-Wilk
PU_mean	4.481	0.427	-0.570	0.164	-0.111	0.326	0.895	< .001
PEOU_mean	4.412	0.485	-0.810	0.164	0.783	0.326	0.896	< .001
TR_mean	4.375	0.484	-1.284	0.164	2.826	0.326	0.899	< .001
PR_mean	4.428	0.475	-1.121	0.164	3.615	0.326	0.884	< .001
HL_mean	3.016	1.519	-0.054	0.164	-1.745	0.326	0.836	< .001
PE_mean	4.483	0.491	-0.480	0.164	-0.645	0.326	0.839	< .001
IU_mean	4.446	0.554	-0.930	0.164	1.073	0.326	0.842	< .001

Source: the table was compiled by author using the software JASP.

Annex 5: H1, H2, H4

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p	Collinearity Statistics	
							Tolerance	VIF
M_0	(Intercept)	4.375	0.033		134.261	< .001		
M_1	(Intercept)	1.919	0.434		4.421	< .001		
	DPC_Total_mean	0.054	0.073	0.049	0.745	.457	0.905	1.105
	PU_mean	0.263	0.074	0.232	3.538	< .001	0.915	1.093
	PEOU_mean	0.234	0.065	0.235	3.587	< .001	0.918	1.089

Source: the table was compiled by author using the software JASP.

Annex 6: H7

Linear Regression

Model Summary - TR_mean

Model	R	R^2	Adjusted R^2	RMSE	R^2 Change	df1	df2	p
M_0	0.000	0.000	0.000	0.484	0.000	0	220	
M_1	0.158	0.025	0.012	0.482	0.025	3	217	.137

Note. M_1 includes DPC_c, HL_c, DPC_x_HL

Source: the table was compiled by author using the software JASP.

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
M_1	Regression	1.294	3	0.431	1.861	.137
	Residual	50.324	217	0.232		
	Total	51.618	220			

Note. M_1 includes DPC_c, HL_c, DPC_x_HL

Note. The intercept model is omitted, as no meaningful information can be shown.

Source: the table was compiled by author using the software JASP.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p	95% CI Lower	95% CI Upper
M_0	(Intercept)	4.375	0.033		134.261	< .001	4.310	4.439
M_1	(Intercept)	4.365	0.033		130.633	< .001	4.299	4.431
	DPC_c	0.143	0.123	0.078	1.165	.245	-0.099	0.385
	HL_c	-0.418	0.257	-0.116	-1.626	.105	-0.924	0.088
	DPC_x_HL	1.448	0.899	0.115	1.611	.109	-0.323	3.219

Source: the table was compiled by author using the software JASP.

Annex 7: H8

Linear Regression

Model Summary - TR_mean

Model	R	R^2	Adjusted R^2	RMSE	R^2 Change	df1	df2	p
M_0	0.000	0.000	0.000	0.484	0.000	0	220	
M_1	0.130	0.017	0.003	0.484	0.017	3	217	.294

Note. M_1 includes DPC_c, PE_c, DPC_x_PE

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
M_1	Regression	0.874	3	0.291	1.246	.294
	Residual	50.744	217	0.234		
	Total	51.618	220			

Note. M_1 includes DPC_c, PE_c, DPC_x_PE

Note. The intercept model is omitted, as no meaningful information can be shown.

Source: the table was compiled by author using the software JASP.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p	95% CI Lower	95% CI Upper
M_0	(Intercept)	4.375	0.033		134.261	< .001	4.310	4.439
M_1	(Intercept)	4.372	0.034		127.064	< .001	4.305	4.440

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p	95% CI	
							Lower	Upper
	DPC_c	0.121	0.126	0.066	0.965	.335	-0.127	0.369
	PE_c	-0.161	0.191	-0.062	-0.846	.398	-0.537	0.215
	DPC_x_PE	0.892	0.640	0.103	1.394	.165	-0.369	2.153

Source: the table was compiled by author using the software JASP.

Annex 8: H3, H5, H10

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p	Collinearity Statistics	
							Tolerance	VIF
M_0	(Intercept)	4.446	0.037		119.331	< .001		
M_1	(Intercept)	1.666	0.469		3.555	< .001		
	PU_mean	0.302	0.086	0.233	3.508	< .001	0.896	1.116
	PEOU_mean	0.110	0.076	0.097	1.458	.146	0.895	1.118
	TR_mean	0.215	0.078	0.188	2.772	.006	0.856	1.168

Source: the table was compiled by author using the software JASP.

Annex 9: H9

Parameter estimates

Direct effects

							95% Confidence Interval	
			Std. estimate	Std. error	z-value	p	Lower	Upper
DSP_Total_mean	→	IU_mean	0.060	0.076	0.792	.428	-0.094	0.205

Direct effects

							95% Confidence Interval	
			Std. estimate	Std. error	z-value	p	Lower	Upper

Note. Estimator is ML.

Source: the table was compiled by author using the software JASP.

Indirect effects

									95% Confidence Interval	
					Std. estimate	Std. error	z-value	p	Lower	Upper
DSP_Total_mean	→	TR_mean	→	IU_mean	0.044	0.022	2.032	.042	0.012	0.104

Note. Estimator is ML.

Source: the table was compiled by author using the software JASP.

Total effects

							95% Confidence Interval	
			Std. estimate	Std. error	z-value	p	Lower	Upper
DSP_Total_mean	→	IU_mean	0.105	0.076	1.384	.166	-0.051	0.248

Note. Estimator is ML.

Source: the table was compiled by author using the software JASP.

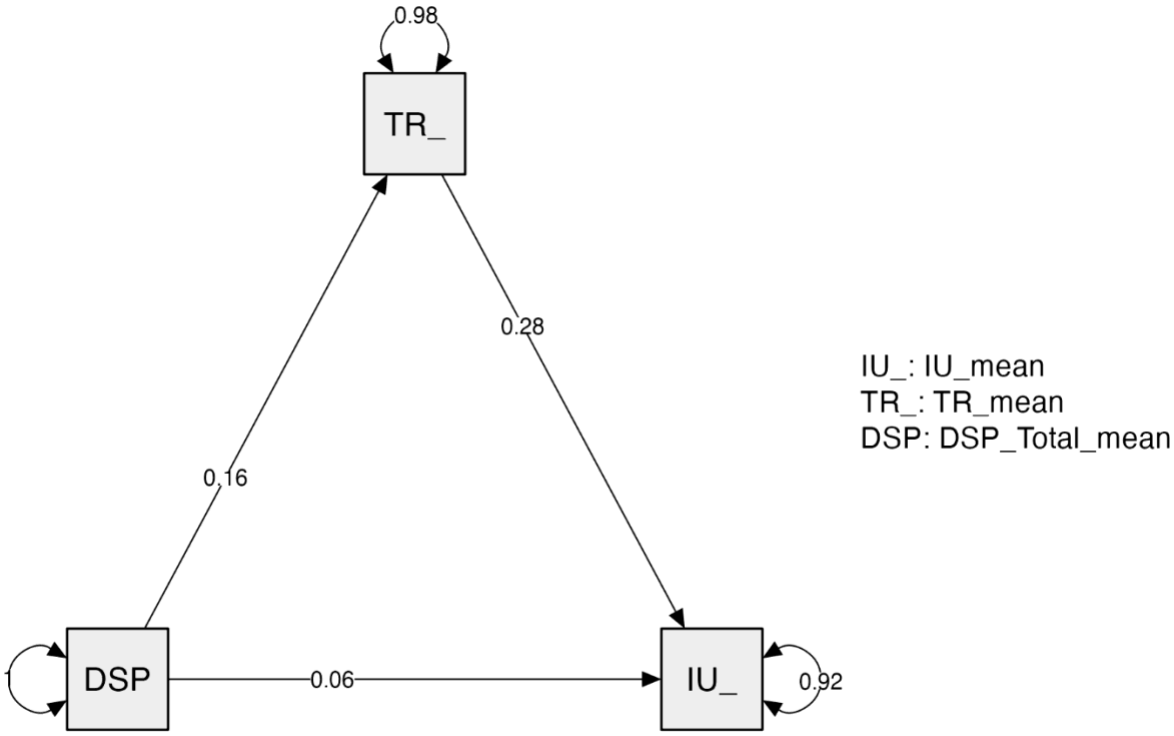
Path coefficients

							95% Confidence Interval	
			Std. estimate	Std. error	z-value	p	Lower	Upper
TR_mean	→	IU_mean	0.275	0.097	2.853	.004	0.094	0.469
DSP_Total_mean	→	IU_mean	0.060	0.076	0.792	.428	-0.094	0.205
DSP_Total_mean	→	TR_mean	0.161	0.076	2.123	.034	0.012	0.313

Note. Estimator is ML.

Source: the table was compiled by author using the software JASP.

Path plot



Source: the table was compiled by author using the software JASP.

Annex 10: H6

Linear Regression

Model Summary - IU_mean

Model	R	R^2	Adjusted R^2	RMSE	R^2 Change	df1	df2	p
M_0	0.000	0.000	0.000	0.554	0.000	0	220	
M_1	0.204	0.041	0.028	0.546	0.041	3	217	.027

Note. M_1 includes TR_c, PR_c, TR_x_PR

Source: the table was compiled by author using the software JASP.

ANOVA

Model		Sum of Squares	df	Mean Square	F	p
M_1	Regression	2.799	3	0.933	3.129	.027
	Residual	64.706	217	0.298		
	Total	67.505	220			

Note. M_1 includes TR_c, PR_c, TR_x_PR

Note. The intercept model is omitted, as no meaningful information can be shown.

Source: the table was compiled by author using the software JASP.

Coefficients

Model		Unstandardized	Standard Error	Standardized	t	p	95% CI	
							Lower	Upper
M_0	(Intercept)	4.446	0.037		119.331	< .001	4.373	4.520
M_1	(Intercept)	4.425	0.038		117.146	< .001	4.351	4.500
	TR_c	0.233	0.129	0.125	1.807	.072	-0.021	0.487
	PR_c	0.646	0.290	0.148	2.230	.027	0.075	1.217
	TR_x_PR	-1.406	0.975	-0.100	-1.442	.151	-3.328	0.515

Source: the table was compiled by author using the software JASP.