KHAZAR UNIVERSITY

Faculty:Graduate School of Economics and Business

Department: Economics and Management

Specialty:Regulation of Economics

MASTER THESIS

ANALYSIS OF THE PROBLEMS OF DIGITAL BANKING REGULATION IN THE MODERN ERA

Applicant:_____ Lala Namig Balajayeva

Supervisor:_____ Ph.D. in Econometrics
Sara Mubariz Huseynova

Baku – 2025

XƏZƏR UNİVERSİTETİ

Fakültə: İqtisadiyyat və Biznes Yüksək Təhsil

Departament:İqtisadiyyat və Menecment

İxtisas:İqtisadiyyatın tənzimlənməsi

MAGİSTR DİSSERTASİYA İŞİ

RƏQƏMSAL BANKÇILIĞIN TƏNZİMLƏNMƏSİ İLƏ BAĞLI PROBLEMLƏRİN MÜASİR DÖVRDƏ TƏHLİLİ

İddiaçı:_____ Lalə Namiq Balacayeva

Elmi rəhbər:_____ i.ü.f.d Sara Mübariz Hüseynova

Bakı – 2025

ABSTRACT

The aim of this dissertation study is to analyze the current regulatory framework in the Republic of Azerbaijan and examine how users perceive the quality and effectiveness of the existing regulation in terms of risk management, personal data protection, consumer rights and trust in digital banking services. This research contributes in a novel way by merging an international theoretical approach on digital banking regulation with empirical evidence from Azerbaijani users, and by blending theoretical components into a legal, technological and institutional context.

I chapter "Introduction" describes the importance of digital banking for the financial system of Azerbaijan, the research problem and gap, the aim, the research questions and hypothesis, as well as the object and subject of the research.

Chapter 2 "Theoretical and Literature Review" analyzes public interest theory, risk- and principle-based regulation, institutional theory and technology acceptance models to explain digital banking regulation. It identifies particular gaps in domestic research surrounding legislative adaptation to fintech, supervisory capacity of digital banking, consumer protection, and open finance.

Chapter 3, Data Analysis introduces a description of the research design and the survey instrument, a description of the sample of 118 users of digital banking services, descriptive statistics, reliability tests, and two multiple regression equations. The results reveal that the success of risk management from the user's viewpoint is dependent on legislation keeping pace with technology and state-bank compliance.

Chapter IV, "Future Prospects of Regulation of Digital Banking in Azerbaijan", situates the findings for the context of Azerbaijan, and it examines challenges such as outdated and incomplete legal frameworks, insufficient transparency and consumer rights protection, and rising cybersecurity threats.

Key words: digital banking, financial regulation, risk management.

TABLE OF CONTENTS

List of acronyms and abbreviations

AI	Artificial Intelligence
AML	Anti-Money Laundering
API	Application Programming Interface
CBDC	Central Bank Digital Currency
CBA	Central Bank of Azerbaijan
CERT	Computer Emergency Response Team
CFPB	Consumer Financial Protection Bureau
DORA	Digital Operational Resilience Act
DLT	Distributed Ledger Technology
EU	European Union
FCA	Financial Conduct Authority
FS-ISAC	Financial Services Information Sharing and Analysis Center
GDPR	General Data Protection Regulation
IMF	International Monetary Fund
ISAC	Information Sharing and Analysis Center
IT	Information Technology
KYC	Know Your Customer
MAS	Monetary Authority of Singapore
PSD2	Second Payment Services Directive
SPSS	Statistical Package for the Social Sciences
TAM	Technology Acceptance Model
UK	United Kingdom
UPI	Unified Payments Interface
US	United States
UTAUT	Unified Theory of Acceptance and Use of Technology

List of Tables

List of Figures

I CHAPTER. INTRODUCTION

1.1. Significance of the study

Modern digital banking is a rich and complex issue that requires consideration of new financial technology, security, and fluctuating economies around the world. The problem is important to consider because as more financial services are provided in a digital space, it is necessary to have progressively stronger regulatory structures in place that nurture security, ensure consumer protection, and maintain a sound system. Banking issues enter the scope of regulation when a bank extends beyond its customary banking activities, e.g. with digital banking, requiring full legal and technological regulation. Regulatory issues also arise for decentralized finance, artificial intelligence banking, cross-border banking and financial services adding to the complexities of how such institutions are regulated. Digital financial banking without proper regulatory frameworks may be used for financial malfeasances and fraud, or may otherwise generate systemic risks to individual users and, in some cases, the entire financial framework on a global scale.

The absence of a common regulatory framework creates openings for regulatory arbitrage by fintech and digital lenders and results in regulatory gaps that could lead to risks for the financial system. The very fast pace of technological innovation means that customary types of regulation lag far behind FinTech innovation and its scale. This results in supervision loopholes that can be exploited by malicious actors. However, the wide divergence in regulatory requirements across jurisdictions, and the fragmented international regulatory cooperation make it challenging to establish an international standard for the regulation of DFS providers. Understanding the differences in the approaches across regions is important to developing harmonized, agile and future-proof types of regulation that adapts to advancements in technology without compromising financial stability. In a digital-payments world, flexible and thorough regulation of the digital banking environment will be needed to provide the type of trust customers expect.

Cybersecurity will remain a huge concern for bank regulation in the digital economy, especially as cybervariouses become more advanced and sticky, and

regulators should also be focused on information and privacy protection and on how cybervariouses affect financial stability of the financial ecosystem as a whole. Because it is a digital banking environment that relies upon the use of cloud computing, artificial intelligence (AI), and blockchain, industry officials say the cybersecurity defenses are needed to protect against vulnerabilities that could leak sensitive information and slow down the entire financial system. Compliance with the strongest cybersecurity standards could help eliminate the risk of large-scale hacks that weaken public trust and disrupt the banking system. Regulators must therefore balance the imposition of controls to improve cybersecurity against the need to ensure financial ease and foster innovation by developing strong yet non-unduly burdensome cybersecurity regimes.

There is also the issue of financial inclusiveness and access to electronic financial services, where electronic banking has the potential to narrow the financial gap and provide access to the unbanked population, but overly stringent regulation would restrict the growth of electronic banking. Compliant requirements can also deter smaller fintech companies from entering the marketplace which may impact competition and innovation. Without an appropriate structure, consumers may be more likely to face fraud, identity theft, or predatory lending as seen in markets with no or weak enforcement. The tough part is writing the rules that allow more financial access, without weakening other protections for consumers or the financial system itself. Technical knowledge of where technology, finance, and rules intersect will be essential to ensuring that this type of research has the biggest impact on the future of banking.

The intersection of customary banking and new actors, such as cryptocurrencies and decentralized finance (DeFi), has created a complex regulatory landscape. They were never designed with a view towards supporting networks that operate in a manner over which no single controlling entity can exercise direct supervision. It has been described as a colossal challenge in terms of legality and policymaking. However, it can also be challenging for regulators and government to see a coherent regulating path, especially about how the new ecosystem weakens

existing financial infrastructure. Where there is no coherent and defined regulating path, financial frauds, tax evasion, and money laundering could all thrive, and the unregulated digital finance could have a more important effect on the financial security and financial stability. As online banking becomes more common, protecting consumers is paramount. Transparency, fairness in lending, and ease of dispute resolution are all essential components of trust in financial institutions. Digital footprints allow institutions to make decisions in real time, thus having an immediate impact on consumers. Many of the providers of these services, especially in the case of the latter, are not sufficiently regulated relative to the type of digital banking services being provided, so legal protections for digital banking consumers are often lacking. Financial literacy is notably low, and users of financial service providers frequently lack the ability to safely use them or recognize scams or predatory lenders. Therefore, rather than only assessing whether digital banks fulfill institutional requirements, there is also an objective to use regulation to actively protect and educate consumers and to achieve a more resilient and equitable financial system.

It is impossible to avoid the geopolitical dimension of regulating banking in the digital age: financial technology is merging with national security. Regulation is particularly challenging as there is competition between regulatory goals and technical capabilities in harmonizing international regulation of data protection, financial surveillance and internet money in crypto currencies. As state governments and networks of cybercrimes exploit weaknesses in banking in a virtual environment for political and financial advantage, regulators also have to coordinate in an international environment to develop harmonized counter-strategies against new and emerging threats. This requires looking at how international institutions can promote harmonization of regulatory regimes for banking in a virtual currency context. As private or state-issued virtual currencies become more prominent, the regulatory framework for these currencies will become more complex. It is vital to pay attention to policy review and reform. The objective of this paper is to examine the technical, legal, economic and geopolitical issues that underlie the various models that can

shape banking regulation in the digital age, through an analysis of the shortcomings of existing models and possible alternatives as part of a broader discussion on how to build a safer, more accessible and more resilient banking landscape in the digital age. As financial technology changes, policy frameworks and regulations need to be re-evaluated and changed, making this a perennial topic of discussion for regulators, financial institutions and citizens.

1.2. Problem setting and learning level

The academic literature on foreign banking regulation has been enormous, including issues of cybersecurity, financial stability, compliance as well as new technology's impact on the financial services industry. Most of this literature has focused with respect to decentralized finance, financial services based on artificial intelligence, cross-country regulatory differences, and similar aspects, and has strongly stressed the need for a flexible and future-sensitive legal framework. There have been comparisons between some countries and in fact there have been detailed discussions about the way developed economies and financial centres approach the regulation of digital banking but in comparison with such a high level of work in such subjects the long-term socio-economic implications of regulatory policies, especially in emerging market economies is still an area where further research is needed.

Fintech issues are new and have so far not been studied extensively in Azerbaijan. Most of the publications on the subject are dedicated to the implementation of fintech solutions and modernization of banking infrastructure. However, in terms of fintech regulation literature, they only refer to technological regulations and do not include legal and economic regulations. The role of consumer protection, financial inclusion, and legal regulation in fintech startups in postdigital banking is not much studied in Azerbaijan. Further research is needed to analyze the effectiveness of existing regulatory instruments, and to design alternative flexible instruments that comply with international standards.

The other area, which is worth investigating on the basis of Azerbaijani studies is an international cooperation in regulation of the electronic banking. The international literature contains several studies on this issue, but in Azerbaijani literature, it is not explored how international agreements or cross-border financial regulation can influence the national legislation. The financial system in Azerbaijan is also subject to international financial governance frameworks. As electronic banking continues to become ever more transboundary, there is need for research that assesses country compliance with global financial governance frameworks and identifies harmonization gaps that obstruct the electronic extension of financial services.

Ethical and legal risks of e-banking (privacy, Internet security, banking fraud, etc.) have been the subject of interest in foreign literature, however, for the first time, they are analyzed in the scientific literature of Azerbaijan. Although many scientific researches have been conducted on cybersecurity measures applied in electronic banks, the provisions of the legal regime of electronic banks in case of information leaks and computer crimes have been studied few times. Future research could examine how artificial intelligence will impact the banking industry, including computerized financial processes and how responsibility for electronic fraud would be determined between customers and their banks.

However, the socio-economic impact of SME digital banking regulation on SMEs in Azerbaijan has not yet been studied in detail. In this regard, a sufficient number of studies in the literature have been conducted on SMEs' access to financial services in the digital era through regulatory policies and its impact on SMEs' development and competitiveness. Research about impacts of regulating banks in a digitally-driven economy on domestic businesses' access to credit markets, payment processing, and compliance is important for regulators to make effective policies. This research gap can help ease the development of regulatory frameworks that improve financial resilience, thereby promoting economic development. Although studies on experimental regulatory environments and regulatory sandboxes and their impact on the development of fintech in countries abroad have matured

considerably, there is no empirical research in the literature about this phenomenon in Azerbaijan. The potential role of experimental regulatory environments and regulatory sandboxes in the development of fintech and financial stability in the Azerbaijani market is new. Future research can also look into experimental regulatory environments in Azerbaijan that would allow for innovation without compromising financial stability, compare successful international examples and apply them to the Azerbaijani financial market, as well as investigate how the country can responsibly develop financial technology.

1.3. Purpose and tasks of the study

The subject of the research is the regulative issue of electronic banking in the new era, the gaps in the current legislation, and proposing a solution to the problem. The goal of the research is to analyze the Azerbaijani and the global environments in this direction through an empirical and qualitative research. The tasks of this study are as follows:

- Conducting a survey study in order to evaluate consumer attitudes towards electronic banking regulations;
- Conducting the statistical analysis using SPSS, identifying trends in regulation and effectiveness;
- Analyzing financial and legal documents in a review of existing regulatory frameworks;
- Comparing the Azerbaijani legislation with the best international practice to identify its gaps and inconsistencies;
- Study and assess the effectiveness of banking cybersecurity policies.
- Researching the trends in the financial and banking field, and how the financial technologies shape them - Assessing the role of the international cooperation in shaping the Azerbaijani regulative environment of digital banking.

1.4. The object and subject of the research

The aim of the research: to study the features and trends of regulatory framework of foreign countries and the Republic of Azerbaijan in the field of digital banking, to develop relevant proposals for improvement. The subject of the research: regulatory regimes applied in the field of digital banking, policy directions and legal regulation.

1.5. Used research methods

This research employs qualitative and quantitative methods to analyze the regulatory landscape for digital banking. It uses statistical analysis of numerical data related to regulation, financial stability, and consumer behavior in digital banking services. The study compares the Azerbaijani digital banking regulations and best practice employed internationally and identifies gaps and areas needing further consideration. Additionally, the research employs survey study to gather data from banking professionals, fintech professionals, and consumers in order to assess perceptions of regulatory difficulties and impacts of financial services on the economy. The multiregression analysis is conducted to measure the impact of regulatory policies and the financial KPIs on the financial market stability and the usage of digital banking. To measure the relationship on the cybersecurity controls, the regulators' compliance and the financial fraud events in the digital banking, the correlation analysis is implemented. The method used to analyze the legal documents, financial laws and policies is called document analysis to find out how supervision has grown and which approach is more effective in digital banking. In processing and analysis of survey data, and for providing correct statistics and reliable output, SPSS software is used. Our study provides a strong, fact-intensive portrait of how digital banking is regulated that we hope will be useful for regulators and financial services policymakers going forward.

II CHAPTER. THEORETICAL AND LITERATURE REVIEW

2.1. Theoretical foundations of digital banking regulation

The banking industry uses such technology to improve efficiency and customer relationship, while redefining their financials. The Digital Finance Strategy of the European Union sets forth a vision for a secure, integrated and competitive digital finance ecosystem for providers and users of financial services. It proposes four objectives to be achieved by 2030 [60]:

(i) removing all fragmentation in the single digital market to create one harmonized operational and regulative environment for the digital single market

(ii) updating existing regulation of financial products and services, so that financial innovation can take place digitally.

(iii) fostering financial innovation with a data basis through creation of an interoperable financial infrastructure (iv) reducing any future risks and overcoming obstacles posed by continuing financial service digitalization

Banks use technology to increase operating efficiency and customer-service capabilities, paralleling the customary engines of financial innovation. Yet finance has a built-in dualism. Financial innovation, driven by technology, is typically followed by a period of financial crisis and instability in a boom and bust sequence, according to Goetzmann (2016). That such a boom and bust sequence happens is a reminder of the danger of unbridled financial innovation, where early success can sometimes hide deeper vulnerabilities [24].

These sources, such as overconfidence in new financial instruments and regulatory capture, would not have been able to avert the financial crises of the past. During the 2008 financial crisis, the demand for collateral rose in the unregulated shadow banking system, which was perfectly correlated with the increase in securitized subprime mortgages. The unregulated nature of the shadow banking system and its rapid ascendance, which challenged commercial banking with no proper controls and no interventions in between, is considered one of the most important causes of the crisis. [26]

Metrick and Tarullo (2021) argue that financial entities not included in a bank but offering a level of financial solidity risk, whatever its form of business, whatever its legal structure, must in proportion to that level of risk, be regulated. Given the increased attention to issues of privacy of information, there is academic interest in proposals to democratize governance of private information in information capitalism, see e.g. Kapczynski (2020) [31]. Financial regulation could be changed through the use of new emerging technology, such as DLT for compliance checking and greater transparency in the tokenized marketplace [5]. Banks are more resilient with sufficiently high capital levels [22; 33]. Aspects of these may have been among the factors behind the severity of the 2008 financial crisis, for instance procyclicality in capital requirements [33]. Banking regulation concern is that minimum requirements merely prevent technical insolvency of a bank, but that only excess capital above these minimum requirements can act as a buffer during a financial downturn [27]. However, this paradox suggests that, while important, capital buffers cannot be the only financial tool to address the financial risk of technological innovation.

Of course, given the two-edged sword nature of financial innovation, the best ways forward will have to be discovered by experimentation with alternatives. As financial technology will evolve, both financial and supervision structures will have to evolve in an attempt to keep pace with such development. One example of an adaptive approach is to use a regulatory sandbox: a testing ground for new financial goods and services that is granted waivers from an entire range of regulative provisions for a limited period of time [2]. This enables the regulators to understand the potential dangers as well as the benefits of regulating a type of financial innovation before creating a permanent general provision, and allows future supervisors to develop hands-on knowledge of regulating a new financial innovation [2].

Financial services are becoming ever more granular, and can be offered in an open model for finance. Based on open finance, an alternative model of financial intermediation is emerging in which standardized products and offerings from banks

are changed and recombined to reflect the needs of the individual [9]. One key agent in the new landscape is the abundance of alternative-business models for fintech companies, with little direct regulatory care. Fintech companies, using the increased demand for financial services in a digital format and for electronic payments, and new, state-of-the-art techniques for processing information (e.g. satellite-powered evaluations of risk), can extend financial decisionmaking and access to credit for disadvantaged people around the world.

Various theories of technology acceptance and diffusion have been applied to the digitalization of financial services. The most important of these frameworks for financial service digitalization are the Theory of Diffusion of Innovations, the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT).

Everett Rogers's Theory of Diffusion of Innovations explains how, why, and at what rate new ideas and technology spread, and may consider relative advantage, compatibility with existing values and practices, simplicity and ease of use, trialability, and observability [46]. The third category is based on the rate of adoption of innovations: innovators, early adopters, early majority, late majority, and laggards [46].

The Technology Acceptance Model (TAM), developed by Fred Davis, states that the only two determinants that will make a technology adopted by its users are its usability and its utility. This means that, according to the TAM, when an individual feels that a computer tool will make financial work easier and that it is easy to use, then such a tool will have a high chance of becoming part of its routine use [17].

The model UTAUT (Unified Theory of Acceptance and Use of Technology) by Venketsah et al. extends the TAM with four integrated constructs which affect the acceptance and usage: performance expectancy, effort expectancy, social influence and easing conditions. This approach is better suited to explaining technology acceptance behavior with respect to a variety of external and psychological determinants in a range of industries including finance [20; 55; 56].

In areas such as electronic payments, mobile banking, and financial services that use fintech innovations, these frameworks can be used to analyze the transition to virtual financial services.

• Mobile banking. The Diffusion of Innovations theory helped explain the adoption of the mobile banking service by considering how well it integrated with users' needs and usage patterns. Where mobile penetration is high and banking is low, its comparative advantage and compatibility spur its high-velocity use. According to TAM and the UTAUT, which focus on ease and perceived use, people will use the mobile banking service when they consider it to be more convenient and efficient to them [45; 54].

• Digital payments. TAM can be applied to measure the acceptance of digital payments, and it shows that perceived ease of use is the most important factor. The social influence component of UTAUT suggests that if one's peer group accepts cashless payment options, one is likely to implement it too. Likewise, if family and companies use it, one is likely to follow suit [20; 38].

• Fintech innovation. Adopting new fintech solutions is difficult, and acceptance of these solutions tends to disrupt customary financial structures. In the TDIF diffusion and adoption models, consumers or early adopters and innovators act as the main drivers in the common diffusion of the technology, while in the UTAUT model the technological infrastructure and government policies are included among the easing conditions and play a fundamental role in the process by which fintech solutions enter the customary financial system [25; 50].

The models discussed here account for the emergence and growth of digital finance, thus promising to provide regulators, entrepreneurs, and researchers with insights into new challenges, help develop more inclusive financial technologies, and create an ecosystem fit for innovation while maintaining security and inclusion for all participants.

Table 1 summarizes the different theories of digital banking regulation and their relevance to designing, improving, and adapting digital banking regulation to

specific needs and challenges. With the evolving landscape of digital banking, these theories can help develop appropriate and effective regulatory frameworks.

Table 2.1.1. Theoretical foundations of digital banking regulation

Theory	Description	Relevance to digital banking regulation
Public interest theory	Regulation is justified to protect the public interest and avoid market failure.	Supports government overseeing digital banks, stressing consumer protections and maintaining financial sector stability
Regulatory capture theory	Postulates that regulators may work to the benefit of industry players rather than the public	Highlights risk of industry capture in digital banking rules, leading to possible loopholes in regulation
Institutional theory	Explores how regulation is shaped by institutions and their norms	It explains diverse approaches to digital banking across jurisdictions and from regulators.
Risk-based regulation	Proponents of these regulatory strategies advocate targeting the areas of highest risk.	Helps regulators to focus their work on cybersecurity, prevent fraud, and protect data.
Principle-based regulation	Prefers broad, principle-based regulations over strict, rule-based compliance	Is open to flexible regulations on digital banking to encourage technological advancements
Law and finance theory	Examines the impact of legal systems on financial development and regulation	Examines the relationship between legal traditions and approaches to regulating digital banking
Financial intermediation theory	Review the role of intermediaries in the financial markets, as well as regulations.	Contributes to understanding of how digital banking regulations shape customary and fintech financial intermediaries
Agency theory	Focuses on the relationship between principals (owners) and agents (managers) within financial institutions	This has been addressed by governance, compliance and accountability frameworks.
The precautionary principle	Recommends regulation even if the potential risk hasn't fully materialized yet.	It supports the proactive and responsive regulation of digital banking for reducing emerging risks such as financial fraud enabled through AI.
Cybersecurity governance framework	Provides a standardized methodology for managing cyber risks in digital financial services	It develops recommendations for data privacy, cybersecurity, and fraud protection and prevention regulations.

Source: The table has been compiled based on [3; 14; 48; 52; 61] by the author.

In this way, these theories form a set of approaches to deal with and shape banking regulation in changing financial realities.

The public interest theory of regulation posits that regulatory standards for financial institutions provide the foundation for the supervision of banks and the financial markets because they serve the public interest in key consumer protection, integrity, and efficiency of financial markets [52]. The theory supports why the government should intervene in the rapid digitization of banking services to avoid systemic instability. Thus, financial markets can be prone to volatility due to poor controls and crises can occur inflicting losses on individuals and the economy.

A particular concern regarding regulation is related to regulatory capture theory, whereby regulators become beholden to the same entities that they have a function to monitor [14]. In fintech banking, many large financial technology companies can have a lot of political and economic clout. A risk is that such companies can help write regulations in a way that favors them at the expense of healthy competition and consumers. It is relevant, however, in cases in which deregulation is used by fintech firms in the name of fostering innovation to weaken consumer protection laws. In the absence of guaranteeing independence and vigilance among regulators, financial regulation is biased against small firms and in favor of big industries.

Based on institutional theory, the legal framework, compliance and innovation rules for the banking sector in a country will be according to the quality of the banking-related institutions. Strong institutions will also make sure that the laws and regulations on the digital banking sector are organized, thus easing compliance and innovation within the new sector. Weak institutions will leave laws on digital banking chaotic. They will limit compliance and innovation. Institutional theory can help understand the hard coordination task of international financial regulating efforts as well as the impact of institutions such as regulating customs and capacities on the development of banking laws and regulating in banking.

Risk-based regulation is therefore practical in attempting to prioritize those areas that best capture the risk of a financial crisis occurring. In banking in general,

and technology banking in particular, this means attempting to regulate cybersecurity, fraud, and anti-money laundering, rather than regulating all financial activities [3]. The benefits of this model are that regulators can save time and not weigh down financial companies with regulations that are not specific to the applicable market. However, new and emerging risks such as financial platforms powered by artificial intelligence (AI) do not necessarily present themselves to regulators, and real-time monitoring and response may be required.

Principle-based regulation is a less prescriptive and more flexible form of regulation. It is not just focused on compliance with inflexible rules, but instead compliance with broader principles. This is especially important for electronic banking, where technology is changing rapidly and where legislation can be out of date almost overnight. Principle-based regulation creates general regulatory objectives, such as consumer protection or financial stability, that regulators can creatively apply to new regulatory problems and new circumstances, even if they do not change the underlying statutes. The effectiveness of principle-based regulation depends, however, on the extent to which regulators are consistent in interpreting and applying the principles, which can cause uncertainty about what compliance entails. Law and finance examines elements of financial regulations suited to different legal systems. This is, at least in part, why the law of electronic banking varies by country. Common law countries tend to regulate through the marketplace model, providing their sectors with a climate of operational flexibility whereas civil law jurisdictions take a stronger approach of preventing economic crime and protecting the consumer; thus, the latter's electronic banking legislation is more aimed at protecting the consumer, and the approach is still followed in creating better environments of innovation.

Financial intermediation theory is an extension of this literature to the new model of banking in a digital era and the changing role of financial intermediaries. Professional banks used to intermediate between lenders and borrowers. However, fintechs have disintermediated the previous banks and provide financial services without the intermediary. Regulations also need to take into account the way in

which participants within any of the models of a digital bank will interact with the customary financial system so they do not threaten financial stability, lead to liquidity runs or spur other forms of lending that fall outside the regulatory perimeter.

Agency theory is also most relevant if the business is a web financial platform or fintech startup, where the goals of the owners of the financial institution and its management may diverge or differ. Thus, transparency and accountability to regulators should be high in these cases. These characteristics can lead management groups to take actions that are short term profit maximizing, but not long term value maximizing, and increase the risk of financial instability. Accordingly, there is a need for laws to impose governance requirements upon companies to align the interests of managers with general investors and consumers.

The precautionary principle looks to the future: it claims that regulators have an obligation to act in anticipation of future harms, even if they are not yet fully confident that this will happen and even if they do not yet know the full dimension of such future risks. In banking in cyberspace, the precautionary principle would require regulators to impose protective controls on anticipated new threats such as financial fraud with AI, unregulated virtual trading in financial assets and information privacy abuse. While such intervention is sometimes seen as over-regulation, it is part of the duty of maintaining financial stability and protecting the welfare of its citizens against unforeseen adverse events. Without it, cyberspace banking systems can easily allow for unnecessary crises in the financial system.

Cybersecurity governance frameworks thus become important in combating emerging threats to electronic banking through cyberattacks and data breaches. As data related to financial transactions is recorded electronically, the regulators have a concern over the security of banking systems. Cybersecurity frameworks provide the financial services sector an established structure to manage its risks, implement the necessary security controls, and appropriately defend against cyber attacks and events. Because cyber threats can evolve rapidly, frameworks need to be reviewed and updated regularly, with active collaboration between regulators, financial

services firms, and technical experts. Collectively, the theoretical models present a well-balanced depiction of the regulatory issue in the digital banking sector, and the regulators can include in policy the suitable components from each model to create a well-balanced strategy that promotes innovation and financial stability, while simultaneously protecting consumers. To meet the challenge posed by digital financial services, a multi-dimensional model that includes risk-based supervision, institutional flexibility, regulatory harmonization, and proactive cybersecurity is needed. A constantly evolving landscape means frameworks must counter that emerging threat, but not stifle the development of new technological advances.

2.2. Literature review on regulation of digital banking challenges

Regulatory issues of fintech and digital banking have been a major research focus in academic literature, including issues such as fintech innovation, technology risk, regulatory compliance, and systemic risk. The landscape for fintech and digital banking regulation keeps developing, with a generally favorable regulatory climate defined by flexible regulatory regimes that strive to balance technology growth against technology risk. There is also a large body of research concerning the impact of the regulation of fintech and digital banks: Cybersecurity, financial inclusion, uncertainty of the law, regulatory culture in promoting and incentivising innovation for stability objectives etc. This section summarizes and critically evaluates the regulatory approaches to fintech and digital banking that have been theorized in the literature over the years and considers their subtleties.

Ofodile et al. (2021) noted that US and Nigeria had different approaches in supporting Fintech development through their paper about comparing the Fintech development regulation of Nigeria and America. Fintech ecosystems with a well-organized regulating environment appeared to be Fintech development friendly by setting up good supervision, according to Ofodile et al. (2021). Likewise, Law (2021) urged that although virtual banking provides financial inclusion, it also creates more attack points for cybercriminals, thus requiring more regulatory actions. In their bibliometric study of durability characteristics of the financial

system, Delle Foglie & Keshminder (2021) argue that proper regulation for a new financial instrument such as SRI sukuk has to balance integration and weaken vulnerabilities in the development and expansion of fintech, especially if the instrument is under the Islamic finance umbrella [18]. The underlying theme across all of this research is that regulators need to set up clear and sensible frameworks that promote innovation while managing risks from increased banking and fintech.

Non-technical aspects of CBDCs have also been studied. For instance, Infante (2021) discusses financial inclusion and the risk of disintermediation to banks in the context of CBDCs [30]. Wadesango et al. (2021) consider the financial transparency of IFRS and find that, theoretically, uniform standards allow for consistent regulation around the world; however, practically, operational realities such as rollout in less resourced countries make this impractical [58]. Ashta and Herrmann (2021) supplemented such discussion via the analysis of fintech in banking by describing both efficiency and access-promoting impact, and new vulnerabilities. They argued that such vulnerabilities required regulatory responses. Altogether, such results indicate a degree of regulatory adaptability and an ability to preserve financial stability, despite new banking business models in a digital age.

Several authors studied the negative externalities of fintech innovations, such as risks related to cybersecurity and concerns regarding privacy. Pereira (2023) analyzed digital tokenization from the perspective of private law and presented an overview that focuses on regulatory gaps regarding the ownership of assets and their transfers [41]. Similar macro studies have since been conducted in India, with Kaur et al. (2019) stating that security concerns are a major barrier to adopting digital banking in Northern India [32]. Supporting this, Eggert (2021) on financial compliance in digital banking concluded that their financial compliance frameworks must become strengthened in an effort to address gaps in business processes [21]. Lee (2024) goes into greater detail about how the digital economy has re-engineered working practices and explores the role of artificial intelligence and the transformative effect of large language models to do so [35]. It recommends that regulators develop effective governance frameworks to make the use of AI in

financial services safe and ethical, even if it produces efficiencies in the related processes. Together, these works suggest a trade-off between security and banking innovation in the digital era, and could point to a need for regulatory policies to maintain security while allowing technological innovation and respecting consumer rights.

An expanding body of work considers the global environment for regulation, including comparing regulatory approaches in different jurisdictions. A fintech regulatory survey, commissioned by the Cambridge Centre for Alternative Finance (2024), found marked differences between jurisdictions that complicate the conduct of cross-border financial activities [11]. Likewise, a study by Pflücke (2024), on open finance & data governance in Europe, found that regulatory regimes conducive to innovation often lack the proper oversight mechanisms to ensure that consumer protection is effective [42]. In a study of bias in financial AI, Chomczyk Penedo and Trigo Kramcsák (2023) found that if regulators implement standardized rules about transparency and fairness, algorithmic bias can be combatted in the European Financial Data Space [12]. All of the above works highlight the fragmented state of the global fintech community and call for international cooperation to level the regulatory playing field of digital banking.

Open finance remains one of the most discussed topics regarding the regulation of digital banking, and academia also studies its potential and related risks. Open finance has, according to Truchet (2024), brought more competition and choice but increased security risks and made regulation for it more of a challenge [53]. This was likewise found by Herrera et al. (2023) in their analysis of the regulation of open finance and development in Latin America and the Caribbean, where they suggest improvements in regulation and a positive outlook for the region but barriers to effective rollout due to infrastructure issues [28]. A third team of authors (Dezem et al., 2023) develops a model for maximizing the use of open banking APIs. They propose a mixed model of in-house and outsourced technology capabilities [19]. Together, the three studies give an overall picture of regulating

open finance, the complex regulatory requirements it entails and the need for flexibility in security and innovation policy.

Big technology's role in financial services has been particularly controversial. Baba et al. (2020) noted that regulatory loopholes allow big technology companies to provide financial services in Europe, while being exempt from many of the regulations that apply to customary financial services providers. Akhtar et al [6]. (2018) studied fintech in development, in North-East and East Asia and stressed the importance of a functional regulatory framework in maintaining market equilibrium [1]. Cornelli et al. (2020) in this regard looked at the fintech and big technology credit markets and observed that such alternative lending has multiplied many times (notably in Asia) [15], which is consistent with Frost et al.'s (2019) observations [15; 23]. The latter has warned that the increasing footprint of the big technology in the financial services could lead to financial concentration and data privacy problems. Regulators face a challenge of balancing the potential for inclusion in financial services that big tech companies bring against the risks they pose to competition and stability.

Yet the question of regulatory adaptation will remain a focus of the next generation of digital banking regulation research. Claessens et al. (2018) identified concerns about the impact of fintech growth on the credit market and cautioned regulators to manage risks and avoid constraining financial innovation [13]. Bazarbash and Beaton (2020) studied the drivers of fintech usages, finding regulatory quality to be a determinant of fintech growth [8]. Buchak et al. (2018) studied fintech in US mortgage lending, highlighting regulatory gaps as a driving force of a new marketplace for mortgages [10].

The studies indicate that financial regulators should work to keep up with evolving financial architectures while safeguarding financial stability and protecting consumers. The academic literature on digital banking regulation stresses the need to balance technology development, risk management, and the design of the regulatory framework. Most experts argue that it is necessary to build regulatory mechanisms to deal with the new issues without creating an obstacle to innovation.

Given the rapid growth of internet bank services, global fintech regulation needs to be adaptive, collaborative and effective. Because of the ever-evolving nature of international finance, with fintechs and digital banking, future research will need to examine regulatory frameworks balancing efficiency, security, and access.

III CHAPTER. DATA ANALYSIS

3.1. Data collection method

We developed a quantitative survey to gain primary data on users' perspectives of digital banking regulation in Azerbaijan. The survey included 21 questions covering demographics, usage behavior, opinions on regulatory effectiveness, and suggestions on how to improve digital banking regulation in Azerbaijan. The survey was prepared with multiple-choice and Likert scale questions about demographic data, technology usage, and the regulatory environment. The survey was distributed via an online questionnaire in a web form. The respondents were the users of digital banking technologies in Azerbaijan. Digital banking users were recruited via social media and email invitation on a voluntary basis, ensuring study participants had experience using digital channels.

Before surveying, the form was tested to ensure the questions were clear (including translations into Azerbaijani) and that the survey's length was appropriate (estimated to be 5 to 7 minutes long). This was done with a small group of respondents. No other adjustments were made, and the survey was distributed. Data collection took two weeks, during which respondents were informed and comforted anonymity was maintained. However, no official information was taken, only an aggregation of subjects' opinion and experience.

The sampling technique used is non-probability convenience sampling to obtain a diverse set of active digital banking users. It is clear not to be a representative sample of the entire population, but it is appropriate to an explorative study, where no pre-formed questions can be formulated, but where instead the range of opinions and trends of actual users is being sought. With 118 valid responses, the sample is adequate for the reliability tests and the regression. This sample may be biased in terms of age, considering that young, more tech-savvy people are more likely to respond to a survey taken online, or in terms of banking habits, with people using internet banking more frequently than those who do not. IBM SPSS Statistics data analysis software was used to enter and analyze the data. Descriptive and inferential statistics were calculated, including frequency analysis, a Cronbach's

alpha test for reliability on all Likert scale items, and multiple linear regression analysis.

To sum up, while the data were collected through a self-administered online questionnaire targeting digital banking users in Azerbaijan due to the availability of respondents throughout the survey period, this is a valid method to assess attitudes and self-reported behaviors while presupposing that respondents provide accurate information and have a good understanding of question wording. The following sections are a description of the sample and a description of the survey results.

3.2. Research participants

The staff survey yielded 118 responses, and the following subsection describes the demographic and other characteristics of the respondents for the purpose of the present study. Tables 1, 2, and 3 show the distribution of the sample by gender, by age, and by education level in order to understand whose views are being measured in these survey data.

Table 1 shows the distribution of participants by gender. Among the 118 participants, 60 participants (50.8%) were female and 58 participants (49.2%) were male.

Table 3.2.1. Gender of respondents

Gender	Frequency	Percentage
Female	60	50.8%
Male	58	49.2%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Because of the approximate balance of male and female respondents, the results may be considered representative of all genders equally as women and men commonly use digital banking in Azerbaijan.

Age. The sample had a relatively younger average age as is typical of users of online banks. Table 2 shows that the age group with the majority of the participants was 25-34 years (31.4%), followed by 35-44 years (26.3%).

Table 3.2.2. Age group of respondents

Age group	Frequency	Percentage
18–24 years	25	21.2%
25–34 years	37	31.4%
35–44 years	31	26.3%
45–54 years	23	19.5%
55 and above	2	1.7%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Most were early/mid-career: 19.5% were aged 45 to 54 years and 1.7% were aged 55 years or older. These cohorts generally adopted less digital banking earlier. This is to be expected as younger people are more likely to use mobile and internet banking as they are more comfortable with technology.

In general, as seen in Table 3.2.3, respondents were well-educated; over half of them had at least a bachelor's degree.

Table 3.2.3. Education level of respondents

Education level	Frequency	Percentage
High school (secondary)	12	10.2%
Technical or college diploma	24	20.3%
Bachelor’s degree	36	30.5%
Master’s degree	38	32.2%
Doctorate or higher	8	6.8%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

More specifically, 30.5% had a Bachelor degree, 32.2% had a Master degree, for a total of 62.7% of the total degrees. In addition, 6.8% had a doctoral degree or higher, 22.3% had tertiary (college) or vocational education, and 10.2% had

secondary education. This suggests that digital banking users in the sample can be characterized as being relatively highly educated. A higher level of education usually leads to a higher level of understanding of financial products, which may have influenced this result on regulations in particular.

In addition to demographics, the survey also asked about the participants' digital banking experiences to provide context:

• As illustrated in Table 3.2.4, the huge majority of respondents mostly use one of the four largest local banks for digital services: Kapital Bank (one third of respondents), ABB (24.6%), PASHA Bank and Leobank (16.9% each). Only a small percentage (6.8%) of respondents stated they bank with an "other bank", which is consistent with the market share in the retail-banking sector. Thus, results of the survey are expected to be representative of the top banks in Azerbaijan.

Table 3.2.4. Primary bank whose digital services are used

Bank	Frequency	Percentage
Kapital Bank	41	34.7%
ABB (International Bank of Azerbaijan)	29	24.6%
PASHA Bank	20	16.9%
Leobank	20	16.9%
Other banks	8	6.8%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

According to Table 3.2.5, the most preferred channel for digital banking was mobile banking, with 36.4% indicating that they benefited the most from such services, and 24.6% from internet banking. Other digital products, such as QR code payments (12.7%), card-based payments (18.6%), and other digital credit products (7.6%) are also used, but by a smaller portion of the respondents. Among the products, mobile banking has the most users. Indicators of quality and functionalities of mobile banking are particularly important, complying with banks' practices and regulatory requirements of security and transparency.

Table 3.2.5. Most frequently used type of digital banking service

Service type	Frequency	Percentage
Mobile banking (mobile app)	43	36.4%
Internet banking (web)	29	24.6%
QR code payments	15	12.7%
Card-based transactions	22	18.6%
Digital loan services	9	7.6%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Experience with issues. Many of the study participants had trouble with the digital banking channels. As shown in Table 3.2.6, 26.3% of users experienced several technical problems, 30.5% a few times and 16.1% just once in the previous six months, and nearly three-quarters of users (72.8%) had experienced a technical problem in the last six months. Elsewhere, only 21.2% said they had never experienced a technical problem, and 5.9% could not say. It can be inferred that, although not all service disruptions or service outages are subject to regulation, the relatively high incidence of service interruptions may signify either operational inefficiencies or inadequacies in the regulation (e.g., lack of focus on supervision, insufficient investment in the infrastructure). Regulators may be able to indirectly influence this by imposing minimum uptime or reporting requirements on banks.

Table 3.2.6. Technical problems experienced in digital banking (last 6 months)

Experience of issues	Frequency	Percentage
Yes, repeatedly (many times)	31	26.3%
Yes, a few times	36	30.5%
Only once	19	16.1%
No, never	25	21.2%
Don’t recall	7	5.9%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

The main motivation to use electronic banking services is convenience i.e. reduction in time spent on banking activities. Based on reasons given by respondents

for making use of a banking service (see Table 3.2.7.), it is clear that the most important reason is "saving time", which was given by 39.8% of respondents. Not wanting to go to a bank branch (15.3%), perceived convenience to transact (17.8%), and lower transaction costs compared with customary banks (17.8%) were the top reasons to adopt cryptocurrency. A small proportion of respondents (9.3%) adopted cryptocurrency for the most private means ("remaining confidential"). These findings fit with international evidence that the key motivations for uptake of digital banking are convenience and cost, and that, since users of digital banking rely heavily on these services, effective regulation is important.

Table 3.2.7. Main reason for using digital banking services

Reason for usage	**Frequency**	**Percentage**
To save time	47	39.8%
To avoid visiting a bank branch	18	15.3%
Convenience/ease of transactions	21	17.8%
Lower service fees	21	17.8%
Privacy (staying confidential)	11	9.3%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

Overall, the users participating in the study were educated, relatively young, considered digital banking to be useful for its convenience and had mostly worked with major banks in Azerbaijan. The fact that most of the users had had at least one technical problem shows that digital banking is not flawless. This contributes to their views on other regulatory aspects, such as regulatory effectiveness, which those experiencing problems may be less likely to perceive positively. The next sections describe respondents' views on regulatory transparency, legal protections, and specific areas of digital banking regulation.

3.3. Research question

Since digital banking is used more and more widely in Azerbaijan, and an adequate level of regulation is required for digital banking systems, the following main research question was defined:

RQ: To what extent does Azerbaijan's regulatory framework for digital banking prove effective, and what modifications can be made to improve the regulation of digital banking within the country?

This general question was subsequently subdivided into a number of sub-questions that the survey was intended to answer:

• RQ1: To what extent do users of digital banking perceive existing digital banking regulations and regulatory authorities to be sufficient and transparent? (For example, are regulatory actions and requirements seen as clear and sufficient?)

RQ2: To what extent do users agree that the current laws and mechanisms are keeping pace with the technological innovations of banking (i.e., do laws keep pace with the growth of digital banking)?

RQ3: Do users believe banks comply fully with the State regulatory framework for digital banking and that the risk management processes in digital banking implement effectively under the regulatory framework?

• RQ4: What do users view as enabling or barring effective risk management and data protection legally, institutionally, technologically, or otherwise in digital banking?

• RQ5: What challenges or problems do users see with the regulation of digital banking, and what steps do they think authorities should prioritize to improve regulation?

Through these questions this research seeks to generate a snapshot of current perceptions and future needs in regulation. In other words, we want to assess how well the regulatory environment is doing now, in the eyes of informed users, and what can be done better. The survey items were created to attempt to gather evidence for each of these categories. The rights items and transparency items were each considered self-explanatory, while the statements on regulation were submitted on a

Likert scale. Question 21 of the survey asked what improvements were most important to the participant.

To answer our research question, we will combine our descriptive results (what do users think of different dimensions of regulation?) with our inferential results (what factors drive perceptions of success or failure in areas such as risk management, data protection, consumer protection, etc.?). This will provide us with actionable recommendations based not just on user perceptions, but also on the underlying reasons, informing the regulatory future of digital banking in Azerbaijan.

3.4. Research hypotheses

These are complemented by the formulation of hypotheses regarding the research question, a literature review, and a contextual analysis that outlines the relationships between the variables in the regulatory environment and their perceived effects on digital banking. The 11 hypotheses reflect the individual variables of the regulatory environment and the items measuring these constructs on the Likert scales of the survey.

H1: The existence of fully developed legal mechanisms for digital banking in Azerbaijan has a meaningful positive effect on the successful implementation of risk management mechanisms in digital banking.

Rationale: If all legal mechanisms in Azerbaijan have been formed ("hüquqi mexanizmlər tam formalaşıb") it is easier to prevent and control the risks of digital banking activities.

H2: The transparency of the work of the regulatory authorities for the users has a positive impact on the successful implementation of the risk control measures.

Rationale: Greater regulatory transparency ("tənzimləyici qurumların fəaliyyəti şəffafdır") is expected to result in better expectations of law compliance and better risk management.

H3: The adaptation of existing legislation to the pace of digital technology development acts as an important catalyst for implementing digital banking risk management mechanisms.

Rationale: When laws keep up with technological change, banks can better address new risks under current rules: qanunvericilik rəqəmsal texnologiyaların inkişaf tempinə uyğunlaşdırılıb.

H4: The full compliance of banks with state normative requirements in the process of providing digital banking services has a positive impact on the efficient implementation of the risk management mechanism.

Rationale: Effective bank regulation and adherence to all legal and normative regulations ("normativ tələblərə tam uyğun fəaliyyət göstərir") cut the levels of risk taken (lack thereof leaves banks vulnerable).

(Hypotheses H1-H4 are all connected to the dependent variable "Risk management mechanisms in digital banking are successfully applied" (survey statement number 15) and the independent variables correspond to each respective survey statement 11-14.)

H5: Effective risk management mechanisms in digital banking positively affect the effective protection of the personal data of digital banking users by law.

Inferred rationale: If risk management (security controls, fraud, etc.) is done well (i.e. "risklərin idarə olunması uğurla tətbiq olunur"), then it is likely that personal data is protected ("şəxsi məlumatlar qanunla effektiv qorunur") because data security is a form of risk management.

H6: Sufficiently high technological security of digital banking systems has a meaningful positive effect on the effective protection of users' personal data.

Rationale: In this statement, "texnoloji təhlükəsizlik yüksək səviyyədə təmin olunur" (strong technical security measures in place), user perception of data protection effectiveness should correspond to the actual security measures in place.

H7: The specialization and training of bank employees in the principles and use of digital services have a positive effect on the effective protection of personal data.

Rationale: Skilled and well-trained staff ("rəqəmsal xidmətlər üzrə əməkdaşları ixtisaslaşmış və təlimlidir") are less likely to make errors or overlook security protocols, thereby improving data protection.

H8: Economic crises are negatively related to the effectiveness of digital banking regulation, as measured by personal data protection. (Conversely, a stable economic environment is related to better regulation in terms of data protection.)

Rationale: If respondents believe economic volatility obstructs regulations, they may be less sure their data is safe. This could be because economic volatility reduces the resources regulators and banks have to ensure proper governance, leading respondents to feel that economic volatility reduces the likelihood of proper governance, and thus, data protection.

H9: Customers' trust in digital banking being a direct function of regulation also has a positive relationship with the perceived effective protection of online users' personal data.

Assumption: Trust (müştərilərin güvəni) depends on regulation (tənzimlələrin səviyyəsindən birbaşan asılıdır). A higher rating for the quality of regulation should also mean a higher rating for the level of trust and a higher rating of data protection. In other words, if the regulation is perceived to be strong, then the protection of personal data (and the trust in that protection) should be rated higher.

(Hypotheses H5-H9 are related to the dependent variable respondents' opinion that "Personal data of individuals using digital banking services is effectively protected by law". The five independent variables are presented in the form of survey statements 15-19, respectively.)

Section 3.6 tests all the hypotheses. H1, H2, H3 and H4 concern whether the impact of any aspect of the regulating environment on the effectiveness of risk management in digital banking is meaningful. H5, H6, H7 and H8 and H9 test whether the impact of any aspect of data protection (the legal protection of personal data) is meaningful. In all cases, these hypotheses posit a positive or negative relationship that could be confirmed or denied by the data.

All hypotheses are framed in terms of concepts that are definitionally subjective and, therefore, the survey items through which they are operationalized elicit a response that agrees or disagrees with the concept. Thus, defining what is meant by a "significant effect" in the analyzes of this paper requires constraining it

to mean that a statistically meaningful association was observed using regression models between the independent variable (the user's agreement with the statement about some regulatory aspect) and the dependent variable (the user's agreement with the outcome statement) while controlling for other variables in the model.

3.5. Limitation

First, it is important to keep in mind the limitations of the study and data before reporting on the results of the hypothesis test:

Sample and Generalizability. Although 118 is a reasonable sample size, it is not random. Using a convenience sample of digital banking users means urban, young and educated people are over-represented, while older and less educated people are under-represented, so findings may not be applicable to the whole of Azerbaijan's population (for example, rural or less technology-motivated people may have dealt with regulation for digital banking differently or not at all). It also means that because respondents come from only a few large banks (Kapital, ABB, Unibank, etc.), findings are more applicable to those banks' digital services' regulation and less so for all available digital services. Smaller banks and non-bank fintech users may report differently.

Self-Reported Perceptions. The survey data is based on self-reported perceptions and opinions. Such data are subjective, and respondents may differ in their knowledge of regulatory transparency and legal protection; whereas some may have personal experience or knowledge by reading, others may have to rely on guesswork. Whether someone has a good or bad experience with their bank can affect their perceptions of the regulatory environment. An unhappy user may attribute a bad experience to regulation. However, this means the data is also intrinsically influenced by perceived performance and not actual regulatory performance. While perceived performance drives user trust and behavior, one must avoid mistaking perception for fact since this can have severe negative consequences.

Cross-sectional Design. The research is cross-sectional; a singular snapshot of time is taken early in 2025. Digital banking is an emerging market in Azerbaijan and its regulation is in its infancy. The 2023 law on payment systems is one promising sign. However, it is not possible to attribute the concerns described above to specific causes or to predict them under a different environment. If those who agree that legislation is up-to-date also have better risk management, we cannot tell whether it is legislation which caused better outcomes or optimists rate everything better. Longitudinal data would allow only to ascertain if causality ran from legislation to improved outcomes, since it would be known which occurred first.

Survey Instrument Constraints. Our survey instrument may not have captured all relevant subtleties. Some statements were ambiguous, such as the "transparency of regulatory bodies" or the "effectiveness of legal mechanisms". These were only assigned to one statement (Q12 and Q11 respectively). Also, there are issues with the Likert scale (1-5) itself: how to define the difference between "agree" and "strongly agree"? In addition to this possible issue with common method bias, it is possible that a person may always be positive (or negative) due to mood or due to how they interpret the scale, inflating correlations between the measures.

Limitations in analysis. The use of multiple regression in hypothesis testing to create perceptual variables does have limitations:

• The independent variables on the left-hand side of the regressions (i.e. Q11-Q14 in the first model) are correlated to some extent, because they all capture the idea of regulatory adequacy. As will be seen, items Q11-Q15 had a very high Cronbach's alpha (0.987), suggesting that they measure a single latent construct. This multicollinearity makes it hard to disentangle which item is the strongest predictor since they share a lot of variance explained.

• There may be other variables that are relevant but were not included in the model, such as demographics. For instance, perhaps things like age or education levels drive views around data protection. However, given our focus and the quite homogeneous sample of active digital banking users, our models remained relatively parsimonious.

• An assumption of linearity is made for the analysis, and Likert scores are treated as if they are continuous numeric variables, though in reality they are ordinal. Despite this limitation, the use of large sample sizes and 5-point scales reduce bias and maintain acceptable standards. The interpretation is not numerically precise, however.

External Factors. The survey does not take into account external influences, such as headlines or events from the past week that may have impacted the respondents. For example, an important cybersecurity incident in digital banking or a critical decision by the Central Bank of Azerbaijan around the time of the survey could impact the responses. No prominent cybersecurity or Central Bank of Azerbaijan incidents occurred during this data collection period. Additional minor factors such as announcements of new fintech regulations or systems outages may have negligible effects on the stock.

In summary, with these limitations in mind the results of this analysis are more useful in highlighting the perceived strengths and weaknesses of digital banking regulation, and ways in which it can be strengthened, than as an audit of the current state of regulation or which approach is the best. As we move to the next part of this text we will be hypothesis testing with these caveats in mind.

3.6. Hypothesis testing

We statistically analyzed our hypotheses H1-H4 (section 3.4) using two multiple linear regression models using SPSS. For both models, we used the statement "Risk management mechanisms in digital banking are successfully applied" (statement 15 from the survey) as the dependent variable and the statements "Legal mechanisms" (statement 11), "Regulatory transparency" (statement 12), "Legislative adaptability" (statement 13), and "Bank compliance" (statement 14) as independent variables. The second regression model tests hypotheses H5 to H9. In this model, the dependent variable is statement 20 of the survey ("Personal data of digital banking users is effectively protected by law"), while the independent variables are statements 15, 16, 17, 18, and 19 corresponding to risk management,

technological security, staff training, economic security, and customer trust, respectively.

Before conducting our regression analyzes, we first checked the reliability of each of the scale item sets and computed basic descriptives.

Reliability of scales: We combined Likert items into two scales:

• Items Q11-Q15 relate to regulatory and risk management issues.

• Q16-20 cover broader challenges and protections within digital banking (technology, people, macro, trust, data security and privacy).

Cronbach's alpha was calculated for each set of items, to check that it was reasonable to add these items together or interpret the set as a single unit. These statistics are presented in Tables 8 and 9, for Q11-Q15 and Q16-Q20 respectively. Both scales have very high reliability ($\alpha > 0.98$), indicating the extent to which the items of each scale tend to be very highly correlated and thus measuring closely related, if not identical, constructs.

Table 3.6.1. Reliability of scale comprising Q11–Q15

Cronbach's Alpha	N of Items
0.987	5

Source: The table has been compiled based on SPSS and survey analysis by the author.

Table 3.6.2. Reliability of scale comprising Q16–Q20

Cronbach's Alpha	N of Items
0.986	5

Source: The table has been compiled based on SPSS and survey analysis by the author.

The alphas are quite high (near 0.99), maybe suggesting redundancy between the items in these subscales (those who agree with one item have an inclination to agree with others). This will be expected. For example, if the respondent thinks that existing legal mechanisms are mature, they may also think that existing laws are keeping up with technology, and vice-versa, possibly leading to multicollinearity in

the regression, as described above. Since the goal is to identify the factors that are truly distinct, we continue and note, in equal measure, that the non-importance of a factor may be due to overlapping variance with another.

Descriptive statistics of variables in hypotheses: Like most regression analysis, you first wanted to know the mean level of support for each survey statement (on a 1-5 scale, where 1 = strongly disagree and 5 = strongly agree). Table 10 (Q11-Q15) and Table 11 (Q16-Q20) provide the means, the observed minimums and maximums (1 and 5, since all options were used by someone), and standard deviations.

Table 3.6.3. Descriptive statistics for Q11–Q15 (regulatory framework & risk management)

Statement (abbreviated)	N	Mean	Std. Dev.
Q11. Legal mechanisms fully formed in Azerbaijan	118	3.05	1.211
Q12. Regulatory bodies' activities are transparent enough	118	3.08	1.295
Q13. Legislation adapted to tech development pace	118	2.82	1.350
Q14. Banks comply fully with state normative requirements	118	3.27	1.312
Q15. Risk management mechanisms are successfully applied (DV in Model 1)	118	3.49	1.279

Source: The table has been compiled based on SPSS and survey analysis by the author.

Table 3.6.4. Descriptive statistics for Q16–Q20 (challenges & protections)

Statement (abbreviated)	N	Mean	Std. Dev.
Q16. Technological security is sufficiently high	118	3.13	1.251
Q17. Staff are specialized and trained in digital services	118	3.07	1.312
Q18. Economic instability negatively affects regulation	118	2.73	1.344
Q19. Customer trust depends directly on regulation level	118	3.64	1.245
Q20. Personal data is effectively protected by law (DV in Model 2)	118	3.43	1.284

Source: The table has been compiled based on SPSS and survey analysis by the author.

• Regulatory framework (Q11-Q14) had a mean of ~3. Overall, 3 was the mean response; Q13, legislation current with technology, was below 3 (slightly disagree). Outcome for model 1 (Q15) resulted in moderate agreement (3.49) that risk management is functional.

• The second set had a mean of 2.73 for Q18. This suggests most respondents do not agree that economic pressure is reducing regulation. They may not have noticed this change, or the environment has not changed sufficiently. Q19 and Q20 have mean scores of 3.64 and 3.43 respectively, indicating that most agree that regulation feeds trust and that current regulations protect personal data fairly well.

• All variables have standard deviations between 1.25 and 1.35, indicating good variation in answers and that all response options are being used.

Regression Model 1 (testing H1-H4) has the dependent variable of Q15 (perceived successful application of risk management) and independent variables of Q11, Q12, Q13, and Q14. The SPSS "Enter" method was used.

The model summary fits with $R = 0.960$ and R-squared = 0.922 to show that the four predictors could explain approximately 92.2% of the variance when perceiving risk management success (Q15). Adjusted $R^2 = 0.919$. Even with these four predictors, the model does a good job at explaining the data here. The R^2 statistic is very high for survey data. The items are very closely related (indeed, they all concern elements of the regulatory environment and, as already pointed out, are very highly correlated). The standard error of estimate equals 0.363 (in original 1-5 scale units). This relates as relatively small to the DV's standard deviation, which totaled about 1.279, indicating a tightly clustered scatter.

An ANOVA for the model produces $F(4, 113) = 334.576$, $p < 0.001$, meaning the model is meaningful and that at least one of the predictors is important in explaining Q15. The R^2 is high so the F-statistic is a large important value.

Table 3.6.5 below consolidates the model fit and ANOVA results for Model 1:

Table 3.6.5. Model 1 fit statistics (DV = Q15, predictors = Q11, Q12, Q13, Q14)

R	R^2	Adjusted R^2	F (df=4,113)	Sig. (F)
0.960	0.922	0.919	334.576	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

***p < 0.001 (model significant).*

Next, we examine the **coefficients** to see the contribution of each independent variable:

- Q11: "Legal mechanisms are fully formed."
- Q12: "Regulatory bodies are transparent."
- Q13: "Legislation is adapted to tech development."
- Q14: "Banks comply with normative requirements."

Table 3.6.6 presents the regression coefficients for Model 1, including unstandardized B, standardized beta, t-values, and significance.

Table 3.6.6. Regression coefficients for Model 1 (Predictors of risk management success)

Predictor (IV)	B (Unstd.)	Std. Error	Beta (Std.)	t	Sig.
(Constant)	0.573	0.100	–	5.721	0.000***
Q11. Legal mechanisms formed	0.037	0.120	0.035	0.311	0.756
Q12. Regulatory bodies transparent	–0.028	0.121	–0.028	–0.232	0.817
Q13. Legislation keeps up with tech	0.375	0.084	0.396	4.464	0.000***
Q14. Banks comply with requirements	0.560	0.090	0.574	6.227	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

***p < 0.001 (significant at 0.1% level).*

• Constant = 0.573: this is an intercept. So with 1 strongly disagreeing about all four Q11-Q14 statements (that is, agreed there is no regulation at all for all four statements), we'd expect answers for Q15: risk management success, to be less than

strongly disagree (an extrapolation, not a category). No one had all 1's and responded meaningfully (a 1 to Q15 too). This constant mainly determines the regression line.

• Q11 (Legal mechanisms): B = 0.037, p = 0.756. Other variables held constant, for each one-point increase in the agreement that "legal mechanisms are fully formed", the perception of risk management success increases by 0.037. This positive influence is minor and statistically non-meaningful. The t-value 0.311 is very low. This means that there is no statistical evidence for H1, namely that the completeness of a general legal framework has a direct influence on the success of risk management.

• Q12 (Regulatory transparency): B = , 0.028, p = 0.817, also non-important; a very small negative coefficient. Hence, this model with banks shows that saying regulators are more transparent does not have any real linear association and that the very small negative association could just be statistical noise. So H2 is not supported. Transparency by itself, when controlling for the other regulatory factors, does not appear to predict perceived risk management success.

• Q13 (Legislation keeps pace with tech): B = 0.375, p = 0.000: A strong positive coefficient indicating that a one point rise in the opinion that the legislative framework is up to date will lead, all other variables held constant, to a 0.375 point rise in the opinion that the risk management system is successful. The corresponding standardized beta for this variable is 0.396. Similar to above, it shows a moderate-to-strong effect (as a high R2 means betas above 0.3 or 0.4 are important). The t-value also indicates importance (4.464, $p<0.001$), so that H3 can be confirmed as perceived flexibility of legislation plays an important role in perceived success of risk management.

• Q14 (Banks comply with requirements): B = 0.560, p = 0.000. This has the largest coefficient and beta. A one-point increase toward agreeing that banks fully comply with risk management policies leads to a 0.560 increase in risk management success. The beta for this variable at 0.574 is relatively big and the most important predictor of risk management success here. t = 6.227 ($p<0.001$): H4 is supported as well, implying that if users perceive banks to be compliant with regulations, they

perceive outcomes (such as risk management) as successful. It might be expected that rule-following banks, subject to the risk controls, would perform better.

The results suggest that in the pooled model, only Q13 (laws are up to date and enforceable) and Q14 (banks are well supervised and regulated) considerably explain perceived risk management ability. In contrast, the other legal variables (Q11, 12) do not. However, legal mechanisms (Q11), and their transparency (Q12), were both closely correlated with Q13 and Q14; those who said there are legal mechanisms also usually said banks are supervised. These may be statistically non-important because they are influenced by Q13/14. The main implication of the estimates is:

• But it's not enough for rules and regulations to be "on the books" or for regulators to applaud transparency if the rules keep up with the pace of innovation, and banks and dealers follow them, risk management is widely viewed as working.

• For example, if banks are compliant (Q14), the existence of a framework (Q11) becomes somewhat less relevant or if laws have been recently updated and are well implemented (Q13) regulator transparency may not be a priority (Q12).

Regression Model 2 (H5-H9): The dependent variable was Q20 (perception that personal data is effectively protected by law). The five independent variables were: Q15 (risk management success, independent variable of model 1), Q16 (tech security sufficient), Q17 (staff training), Q18 (impact of economic instability), and Q19 (trust depends on regulation). All predictors were simultaneously entered into a standard linear regression.

Again, the fit of the model is quite good ($R = 0.970$, $R^2 = 0.941$, and adjusted $R^2 = 0.938$). Thus, these five factors explain 94.1% of the variance of perceived data protection. This is even higher than model 1. These factors almost completely explain how people feel about data protection. This is plausible as Q20 is connected to some of these factors. For example, the success of risk management and trust in regulation would lead to data being perceived as protected. The overall model is meaningful, with F-statistic = 355.465 (df = 5, 112), $p < 0.001$.

Table 3.6.7. Model 2 fit statistics (DV = Q20, predictors = Q15, Q16, Q17, Q18, Q19)

R	R^2	Adjusted R^2	F (df=5,112)	Sig. (F)
0.970	0.941	0.938	355.465	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

***p < 0.001 (model significant).*

Now the coefficients for each predictor in Model 2 are given in Table 15:

Table 3.6.8. Regression coefficients for Model 2 (Predictors of personal data protection)

Predictor (IV)	B (Unstd.)	Std. Error	Beta (Std.)	t	Sig.
(Constant)	0.155	0.105	–	1.476	0.143
Q15. Risk management success	0.205	0.099	0.204	2.079	0.040*
Q16. Technological security high	0.190	0.101	0.185	1.880	0.063
Q17. Staff specialized & trained	–0.026	0.101	–0.026	–0.252	0.801
Q18. Economic instability affects neg	0.273	0.073	0.286	3.750	0.000***
Q19. Trust depends on regulation	0.358	0.092	0.347	3.911	0.000***

Source: The table has been compiled based on SPSS and survey analysis by the author.

*p < 0.05, **p < 0.001*.

• Intercept = 0.155, p = 0.143: Statistically not different from zero. So if a respondent rated all five predictor variables negatively (i.e. they are very pessimistic: they see no RM, no security, all staff untrained, the economy does not harm them, and do not trust people are not affected by regulation), the predicted baseline agreement level about their information being protected would be 0.155, which is basically zero (the intercept is below 1 on the scale), so the intercept is not important.

• Q15 (Risk management success): B = 0.205, p = 0.040. This positive relationship is statistically important at p < 0.05. The standardized regression coefficient of 0.204 indicates a medium effect size and supports the fifth hypothesis

(H5) that officers are more sure that their data is secure if they think that risk management mechanisms are in place and effective. This is still true controlling for other factors in the model. This supports the theory that improved risk management (i.e., fraud prevention, internal controls) likely improves confidence in data protection in this context.

• Q16 (Technological security): B = 0.190, p = 0.063. This is a positive but only marginally meaningful coefficient. As beta is 0.185, which is borderline, we can see that there is some influence, (and there appears to be a correlation since Q16 correlates with Q20), but it is not strong enough to be meaningful at the 95% confidence level. Although evidence was found to support H6, we cannot be as certain as with the effect of perceived tech security on data protection (the effect was not important once controls were included). One possible explanation is that the effect of tech security is through risk management (i.e. tech security contributes to risk management, with successful risk management leading to data protection). Thus we might have absorbed the effect of Q16 through having Q15 as a predictor.

• Q17 (Staff training): B = -0.026, p = 0.801, statistically non-meaningful (effectively 0). This indicates that whether or not respondents think bank employees are well trained had no linear impact on their data protection ratings. H7 is not supported. This is interesting. This could be that staff knowledge is not seen as relevant for data protection, perhaps technology or process are seen as more important, or all banks' staff are similar. However the negative sign may just be noise as it was not statistically important.

• Q18 (Negative impact of economic instability): B = 0.273, p = 0.000. Counter-intuitive, at first glance. If the coefficient were positive, it would mean that higher agreement with the idea that economic instability negatively impacts regulation also meant stronger agreement that the data is also well-protected. However, if high agreement with Q18 means this isn't true. The value itself is somewhat inconceivable, but in practical terms, a beta of 0.286 is a large effect. Alternatively, those who know there are macroeconomic risks may be more likely to support protection. In either case, this could also be because of a suppression

effect, whereby the other variables are so correlated that the residual variance of Q18 is positively correlated with Q20. Despite this, the H8 hypothesis that instability negatively affects regulation, as the H8 statement reads: "instability negatively affects regulation", received a positive coefficient when accounting for all the other control variables. As worded in the survey, if one accepts the idea that economic instability impedes regulation, one might also be more likely to feel that data protection is present. As agreement with Q18 seems to suggest an overall critical viewpoint, one might predict that agreement with Q18 would also mean agreement with a statement criticizing data protection. However, this is not true in the survey. This may be due to multicollinearity, or this may just be due to the way in which the questions have been perceived. In either case, H8 (i.e., the negative impact of instability) is not supported, and a positive effect is found for the idea that framing economic issues as an issue leads to believing that it is obvious how the data is protected. This counterintuitive finding will be dealt with in the discussion.

• Q19 (Customer trust depends on regulation): B = 0.358, p = 0.000. This is a strong, meaningful positive effect. The same question yields a beta estimate of 0.347, t ~3.911, suggesting that respondents who believe that trust in digital banking depends on regulatory quality are more likely to believe that current law protects personal data. This supports H9: Higher perception of the importance of regulation for trust is associated with higher confidence in outcomes of regulation (e.g. data protected). Intuitively: If people think that regulation is important, and presumably if they have high trust it means they think regulation is doing an OK job, thus they will say the data is protected. This factor (Q19) had one of the higher means, and public trust was clearly seen as closely related to effective regulation by the users involved.

• H5: Supported - if risk management is successful, data protection is also perceived as successful.

• H6: Not supported - tech security by itself did not considerably predict data protection when controlling for other variables.

• H7: Not supported - Staff training had no important effect on their perception of data protection.

• H8: Not supported in expected direction - no negative correlation between instability and protection but positive correlation. Further interpretation needed.

• H9: Supported - those who tie customer trust to regulation also advocate that, within regulation, data protection is effective (which indicates that regulation is doing its job).

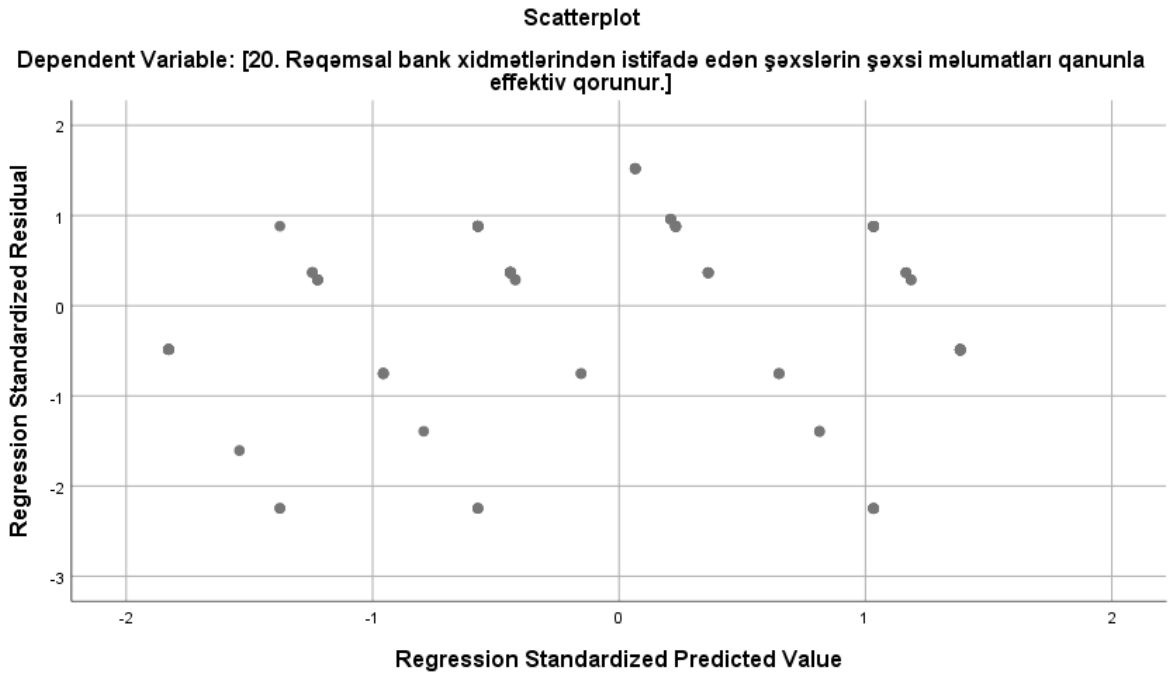
Q15 is a direct risk management factor (moderate in Model 2), indicating a reciprocal influence between (often internal) risk management and its specific data security-related aspects (e.g. legal obligations). Meanwhile, those public and trust factors (Q18, Q19) affect user perceptions of security, while internal factors in the bank, such as the staff (Q17), have little effect.

Assumption checks: Because the very high R^2 values indicate a good fit, we examined the residuals to verify that our models did not violate assumptions.

• Linearity: The relationships appear linear because we used Likert scales (which are approximately interval measures) and there was no need to include any polynomial terms in the models (the residuals vs. predicted scatterplots show no signs of curvature).

• Homogeneity of variance: The standardized residuals were plotted against the standardized predicted values, and the plot of the Model 2 residuals shown in Figure 1 was typical. Predictions were symmetrically distributed around zero, with no funnel shapes or outliers visible, suggesting the relationship between the errors and the fitted predictions is homoscedastic. The variance of the residuals neither increased nor decreased with increasing levels of the fitted scores; likewise, most standardized residuals fell between -2 and +2, suggesting a relatively constant variance. There is no clear heteroscedasticity in Figure 1 (standardized residuals vs. fitted values of Model 2), i.e., the residual variation does not change with data protection perception values predicted by the model. The zero-residual line is indicated in red and the points do not show any trend.

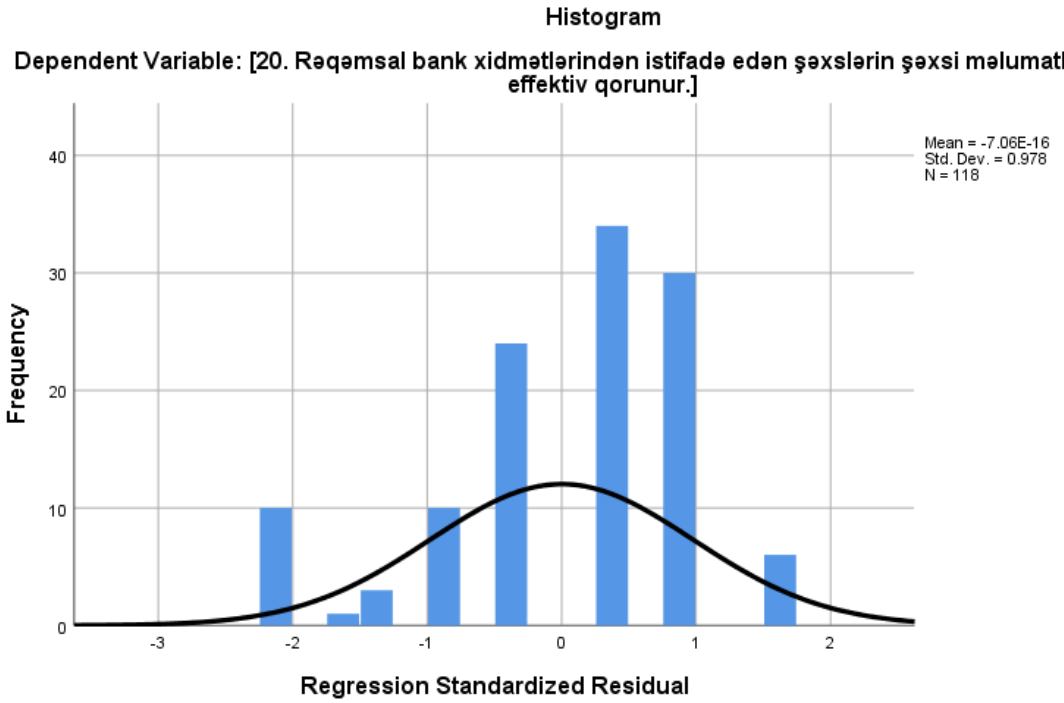
Figure 3.6.1. Scatterplot.



Source: The figure has been compiled based on SPSS and survey analysis by the author.

• Normality of residuals: The histogram of residuals shown in Figure 3.6.2 was approximately normal, with an effectively 0 mean and slight skewness not severe. The histogram of standardized residuals shown in Figure 2 was overlaid with a red normal curve. The resulting distribution looks approximately normal, with most values close to 0 and tails approximately symmetric, suggesting that the regression estimates and importance test results are reliable (and that the normality assumption for the error terms holds).

Figure 3.6.2. Histogram



Source: The figure has been compiled based on SPSS and survey analysis by the author.

Furthermore, for example in Model 1, Q11 intercorrelates with Q12, Q13, and Q14 which results in multicollinearity. We calculated VIFs informally. Obviously, a model with such a high R^2 entails high VIFs. However, since the aim of this analysis is exploratory, and the independent variables are different (conceptual) pieces, we did not exclude any. The lack of importance of some predictors (Q11, Q12, Q17) might also be due to multicollinearity, in which case the inclusion of these variables makes it impossible to single them out from the other items. In any case, we could average highly collinear items (e.g., Q11-Q14 into an index measuring the level of "regulatory adequacy"), but here we want to study them separately.

Overall the regression testing process proved to be successful, with clearly identifiable and important factors that influenced it:

• For effective risk management (Regulatory outcome 1), the determinants were adaptive legislation and strict bank compliance. General legal infrastructure and bank willingness to cooperate were no longer meaningful.

• For data protection (Regulatory outcome 2), factors relevant to users include general trust in regulation, effectively managing risks, and to a lesser extent, perception of economic context. Factors affecting banks' technical and human resources are important to practice in keeping data secure, but not in users' minds when it comes to feeling their data is protected by law.

We consider the implications of these findings for the Azerbaijani case, and for broader regulatory efforts in the future.

3.7. Results and interpretation

Next, we present the quantitative results of the survey. This section presents both descriptive (i.e. responses and means) and inferential (i.e. regression analysis) results of survey responses of digital bank users in Azerbaijan regarding the country's national regulatory framework. The section proceeds to analyze the quality of the Azerbaijan national regulatory framework, based on survey responses.

Perceptions of transparency and legal adequacy: The survey included a direct question about whether respondents thought that regulation of digital banking is sufficiently transparent in Azerbaijan. Responses included three categories.

• Only 21.2% (7.6% "fully transparent"; 13.6% "mostly transparent") of respondents said regulations are mostly or fully transparent (Q8).

• Almost half (46.6%) felt that it was indeed not transparent (at "very weakly transparent" - 28.0% and "not at all transparent" - 18.6%); a third (approx. 32%) felt that it was "partially transparent".

This suggests that the user does not feel that the regulatory processes and communications are open and transparent enough. The user may feel that the Central Bank or other regulators do not publicize rules or changes well, or that banks' compliance or handling of problems is not visible enough. But this lack of transparency can lead to distrust or uncertainty from consumers. In developing

financial systems there may be rules in place, but if they are not clearly communicated or enforced, they may not be trusted by the public.

For regulatory bodies (Q12: "Regulatory bodies' activities are transparent for users"), the overall opinion was slightly more positive (mean rating 3.08, or 41.6% of respondents agreed to some extent). However, this could be due to different wording or possibly the context of the statements. One possibility is that when asked questions like Q8, people are answering about overall transparency of regulation (law-making etc.) while questions like Q12 are considered in terms of the transparency of banking supervision in practice, on a day-to-day basis. However, transparency does not predict success in the regression analysis: it is an important issue but not the overriding factor as far as the indicators are concerned.

User rights and legal protection: In Q10, we gauged how well users' rights are protected in the digital banking domain:

• 29.7% indicated user rights were mostly or fully protected (11.9% "fully", 17.8% "mostly").

• Conversely, 43.2% do not believe protection is well-established (23.7% "weakly protected", 19.5% "not protected") and 27.1% believe they are "partially protected".

It shows that many users are not confident the regulators are protecting their rights (which may include privacy, fair treatment, redress, etc.) in the context of digital banking. This is a problem if you have almost half the users saying they are not confident their rights are being protected, because that means either there is not enough enforcement action, or at least not enough communication on the part of the regulators. It may also be a symptom of problems at the individual level, such as finding it hard to escalate problems or uncertainty over who to report online grievances to. Getting consumer protection is fundamental to good regulation. Such perceptions are, therefore, a concern to both regulators and banks.

Legal framework and regulatory mechanisms: The Likert scale statements Q11-Q15 cover the following regulatory and legal aspects from the perspective of users:

• Legal mechanisms fully in place (Q11): With an average value of 3.05 and a split between disagreeing (33.9%) and agreeing (35.6%), this statement received mixed responses. Generally, a third of respondents believe that Azerbaijan has already adopted legal measures required for the provision of digital banking services, while another third do not. This ambivalence may reflect the legal framework's potential status as work-in-progress; legislatively sufficient for certain stakeholders, but not convincingly complete in the eyes of other stakeholders. Azerbaijan had previously possessed legislation on banking law and e-commerce. However, until recently, there was a lack of legislation covering fintech/digital banking (such as emoney, open banking, and payment institutions). The 2023 Payment Services and Systems Law also helps fill in regulatory gaps (e.g. introducing regulation for e-money, payment institutions, etc) [62]: some respondents may have been remembering the previous time period, before such regulations had entered into force (hence disagree), while others may be aware of recent developments (hence somewhat agree).

• Regulatory transparency (Q12): mean of ~3.08 indicates somewhat more leaning to agree (41.6% agree, 33.9% disagree). This suggests that at the operational level, a considerable number of users perceive that the regulators, e.g., the Financial Services Authority or the Central Bank, take visible actions. People may have heard pronouncements or rules from the news about finances read out loud, but that doesn't represent a solid agreement. Only 15% strongly agreed that it's transparent.

• Legislation keeping pace (Q13): This had the lowest mean score (2.82). The largest proportion of respondents thought that laws are not keeping up with technological change (45.7% disagree, 33.9% agree). (Whilst this is not a majority, it is indicative.) Digital banking covers rapidly evolving tech (online and mobile apps, emerging fintechs etc). If the law is slow to adapt, new services may operate in a legal grey zone or under old law. Respondents all seem to believe there is a delay, which is likely true. For example, till 2023, Azerbaijan had no payment providers nor any law on open banking. Likewise, legislation in developed markets is updated (e.g., EU PSD2 written in the late 2010s for Fintech) and users around

the world know of these trends and may view Azerbaijan as falling behind. The effect of this item is large and important, which reinforces the notion that this is important for users concerned about risk management.

• Banks' compliance with requirements (Q14): A mean score of 3.27 and 47.5% (21.2% strongly agree) indicates this is also a relatively positive response. It seems that a slight majority think banks are largely complying with what the government/regulators ask of them in respect to digital. 28.8% disagree with the statement, which is by no means an insignificant proportion, and they might have seen security breaches. Maybe they heard about banks pushing the envelope (sometimes literally!). It's encouraging that so many respondents don't see compliance as a major issue. If anything, this increases the likelihood that Q14 is the most important variable determining the success of banks' risk management processes. Where people think that banks follow the rules, they think that things work better. This is intuitively obvious; if banks comply with rules, there will be fewer problems.

• Management of risks associated with digital banking (Q15): With a mean of 3.49, this indicates majority agreement (52.5%) at least somewhat agree risks associated with digital banking are being managed. Even though there are legal complexities and transparency concerns, it appears digital banking, in practice for many, is functioning satisfactorily most of the time. (As in the Q6 technical problems question, which most people rarely face, and a minority often experienced problems, which were sometimes self-reported by banks for regulatory reasons). So, this may be partly due to banks' own anti-fraud measures, some regulatory and some voluntary or even other security features. It is a good sign. Whatever the flaws, most people do generally believe that the risk (of fraud / hacking, etc.) is not endemic, or the score for Q15 would have been lower. Indeed, Azerbaijani banks have made recent investments in security (one study points out banks embracing cybersecurity measures [63]), which seems to have paid off.

Technology, staff, and external factors: The second set of Likert items (Q16 to Q20) captured:

• Technological Security (Q16): Mean 3.13, somewhat disagree (33.9%). The security of the technology that supports the digital bank systems is somewhat mixed in terms of customer perceptions. 33.9% of the respondents don't trust the technology (4.19% and 5). News about cyberattacks has become so common that it's understandable if people don't believe it. Locally, people would have no trouble believing if they haven't seen a breach, they're just timid, or have only seen smaller shared network glitches. The overall somewhat neutral report does indicate that this could be an area for improvement or at least more communication to help users feel safe. If we were to look at the regression analysis, Q16 had a very slight impact on feeling that their data is being protected (indicating that while people who see high tech security, tend to feel data is protected, this is not a strong stand-alone factor when trust and risk perception is accounted for).

• Staff expertise (Q17): Mean 3.07. Same distribution. ~41.5% agree that bank employees dealing with digital services are qualified and trained to help, ~35.6% disagree. Though, to be fair, that may not be the most positive of endorsements when it comes to staff competence, given that most users will have dealt with the call center or support worker for digital banking problems and found them not very helpful or knowledgeable. Other people may not have these problems. The human part (supporting the apps, the agents' knowledge) still plays a huge role, and users believe some banks clearly do not provide sufficient training. In our regression, this factor had no impact on perceptions of data safety. It may be that customers consider data protection mainly a systems and rules issue, and that staff quality is very much a separate issue.

• Economic instability impact (Q18): Mean 2.73, most disagree. Most disagree that macroeconomic instability is affecting digital banking regulation, suggesting that at the time of the survey, macroeconomic instability was not regarded as a major barrier to regulating digital banking. Azerbaijani inflation and oil-related boom and bust cycles are not wild like in some economies. Perhaps people thought, "No, even if the economy is shaky, digital banking can be regulated; one doesn't directly mess up the other." Or perhaps they were asked, "Have the crises hurt the online banking

services of banks?" and many people say they have not. Nonetheless, 29.7% agree the economic instability is a problem even for that. Perhaps they remembered some of the banking crises, for example the 2010s mid-decade devaluation of the Azerbaijan manat, which did considerable damage. This is also in contradistinction to the positive coefficient of the regression weight: those aware of macro risks may also pay attention to protection such as this, perhaps a set of informed users who both "worry but also appreciate": that instability could threaten regulation, but that despite the instability their data is safe. In other words, they might strongly agree with both statements.

• Trust depends on regulation (Q19): Mean 3.64, the highest of any item. When asked whether their trust in digital banking depended on regulation, 54.2% (33.9% strongly) agreed. However, only 17.8% of respondents disagreed. This suggests that regulation matters: people do not feel comfortable using digital banking unless they can trust that the regulation will be effective. This is a strong message to regulators. Any compromise in the quality of regulation can weaken public trust and cause slow adoption of digital finance. If regulation is clear and strong, people will make use of this information. That is why Q19 is important in our model, because those who say regulation is strong also tend to say it does a decent job of protecting the data. It is somewhat of a self-reinforcing belief: if I think regulation is important for trust, I either see it enough to trust it is working for my data's safety.

Data effectively protected (Q20): the average score for question Q20 (mean = 3.43) shows that 52.5% of respondents agreed to some degree that personal data is effectively protected by existing laws, while 25.4% disagreed. So slightly more than half feel like the law (data protection laws, bank secrecy, etc.) is providing protection for their data. This seems not to be consistent with the above issues with user rights (Q10 was a more pessimistic question). But, keep in mind, Q20 was asked in a positive phrasing and they might very well have thought that they were saying: "Yes, there is a law on personal data and banks do tell us they protect privacy" (and there is a Law on Personal Data and banks are subject to professional secrecy). While not

perfect, this could indicate that messages about data being protected (for instance from banks, or via regulatory requirements for encryption) have had some positive effect. However, with about a quarter unconvinced, there is still a trust gap for an important minority. Our regression analysis also illuminated who was more likely to find themselves in that unconvinced quarter, and these are people who do not see risk management working, or who do not tie trust to regulation.

The regressions do a good job of capturing the perceived drivers behind the two outcomes of interest: success on risk management and data protection. In other words:

Banks only manage risk effectively if the legal framework is up-to-date and the banks comply with it. If either of the two conditions are violated, users assume the risk is not being managed. It didn't matter as much whether the regulators are super transparent or whether the framework exists in theory - what mattered is practical currency and compliance. So I think that really is what people care about - whether the rules are current. Are they being obeyed? When conditions are met, customers likely see fewer incidents and therefore trust the system.

• We found that people feel their data is safe when they trust the regulatory regime (implying that regulation is key to trust), when they see banks' risk management working (the technical/operational side is required to be working) and interestingly when they acknowledge macro risks (possibly suggesting an advanced view in the regulatory effort). People do not appear to have data security as an explicit consideration of whether staff are well trained or the technology is secure as that is likely reflected in risk management. Instead, it's a holistic assessment: "Overall, I trust the regulators and banks, so I think my data is safe."

These results in particular reflect the realities in Azerbaijan in regards to the aforementioned.

• There are no refined regulations for digital banking in Azerbaijan, and the survey took place in May 2025. At that time, there was a PS (Payment Services) law adopted (in 2023). However, it had not yet taken effect. There was not any digital banking act yet or open banking regulations such as the EU's PSD2, with

open banking pilots starting to happen. The Central Bank is developing a SupTech Roadmap [64] (supervisor technology roadmap). This shows a willingness to embrace the need for regulators to keep apace with innovation, but from the user perspective that has yet to impart confidence in up-to-date law, hence the importance of the Central Bank's aim. This suggests a lack of knowledge as updating legislation was the most requested improvement (Q21) to address these issues.

• Enforcement and compliance seem relatively decent in practice, as people think banks comply and think risk management works. The banking sector in Azerbaijan was cleaned up after the banking crisis in 2015-16, with non-compliant banks closed. Some 26 banks are still in operation under the supervision of the Central Bank, perhaps because the remaining banks comply with regulations. The big players have invested in their digital infrastructure, and comply with rules concerning digital security. User experience has been mostly safe (few have been victims of fraud or data loss, it appears), thanks to the banks and the basic rules set down by regulators. However, compliance needs are ever-evolving, as new fintech products emerge which banks will need to comply with, and this also goes back to legislation adaptability.

• Lack of transparency can also apply to the regulatory changes being published on official gazettes or the Central Bank's website in a manner that is not clear to consumers. Furthermore, members of the public may not be aware of their rights or the process for lodging a complaint. For example, if a digital bank scams a member of the public over the telephone, how would they find out if there is an ombudsman or regulatory framework that empowers them to get their money back? In order to combat the "not transparent" narrative, Azerbaijan could helpfully publish messages using mechanisms such as alerts or information campaigns, as is done in other countries, on digital financial rights.

• Trust also operates in the cultural/normative domain: in a transitional economy, citizens' concern is institutions. People are more secure when the state has strong regulators and less secure when the state has weak regulators. Because some banks failed and people lost their money, citizens of Azerbaijan, where the banking

crisis occurred, might logically assume that lack of oversight has resulted in the loss of money and expect oversight for any new service, including banking services provided by digital networks. Trust regulation (Q19) is highly valued alongside memory, and the exercise of rational caution.

Suggestions for improvement: the last question (Q21) of the survey asked respondents to name what main step should be taken to improve digital banking regulation in Azerbaijan. Table 16 below summarizes the responses. They are consistent with many of the above findings.

• The most preferred choice (33.1%) was to update relevant legislation, seemingly connected with the response to Q13, suggesting that users want the laws refreshed. Whether it was new law for digital banks, closing loopholes in law, or applying existing law to fintechs, nothing was more important, and it was the answer that got one third of all responses.

• The second most popular response (21.2%) was that regulatory authorities should better supervise regulated entities' compliance with regulations (also called 'better supervision'). In addition to better laws, people want regulators to enforce the laws through on-site inspections, audits, and penalties. This ties in with our regression finding that people who relied on compliance most strongly are most likely to think that increased monitoring would force the banks to comply. Perhaps the idea is that more transparency in regulators through active monitoring makes the public trust the regulators more.

The list included investing in digital security technologies (16.1%), public campaigns to raise awareness of online risks (17.8%), and further training of bank employees (11.9%). The difference for this was that investing in security technology fits with the desire for high technological security (links to Q16). Public education campaigns ("maarifləndirmə kampaniyaları") could address the transparency/financial literacy issue: if users are taught how to use digital banking safely and know their rights, it would reduce misuse and increase trust. Continuous training of staff, at ~12%, is a common request from the group of customers. This

group perhaps experienced unhelpful service from staff when they asked for help to use digital services and realized that banks need to upskill their staff.

Table 3.7.1. Top suggested steps to improve digital banking regulation (Q21 results)

Suggested Improvement	Frequency	Percentage
a) Update the relevant legislation	39	33.1%
b) Strengthen monitoring by regulators	25	21.2%
c) Invest in digital security technologies	19	16.1%
d) Run education campaigns for users	21	17.8%
e) Continuously train bank staff	14	11.9%
Total	**118**	**100.0%**

Source: The table has been compiled based on SPSS and survey analysis by the author.

These suggestions reflect the priorities highlighted previously. Legal and enforcement matters comprise the most common category (over 50%), then technology and human factors respectively. This indicates where policy action is needed: a need to modernize laws; active oversight of existing legislation and enforcement activities; and investment in supporting measures (technology, education, training).

Conclusion of analysis: The data analysis, coupled with user ratings, tells a mixed story. Users are reasonably confident about the safety of digital banking (most risks are covered, data is mostly protected), but not about the regulatory environment (laws are lagging, regulators can be more transparent, and the regulatory setup needs improvement). Safety fundamentals are there, partly thanks to individual banks doing their job. To increase user trust and grow digital banking overall in the country, Azerbaijan must shore up its regulatory environment.

Key takeaways:

• Trust and regulation are close: Trust is closely tied to good regulation, and people currently seem to trust regulators fairly well (at least in part because of their ratings on outcomes). This trust could erode if regulation does not keep up from a technological or enforcement point of view.

• Legal reform is also needed. Users are demanding that "regulators and legislators need to catch up with technology". This could include open banking, fintech licensing framework, improved e-signature laws, e-documents, and consumer protection laws for digital services, cybersecurity laws (such as mandatory cybersecurity standards). The new payment law was a good start but we also need to consider new chapters on digital banking provisions in the banking law or adopting international best practices.

• Enforcement and monitoring need visibility: It is important that enforcement and monitoring actions are visible. This means that when enforcement action is taken against a bank that fails to meet its obligations in relation to its digital services, the relevant authority should seek to publicize that enforcement action.

• Consumer-centered measures: while user education is relatively low (17.8%), almost one-fifth of users are aware that many problems could be solved with educating users. A financially literate user base means a less risky user base (less likely to be phished etc.) and users who know their rights (and can hold banks responsible). Regulators in many countries run public awareness campaigns and this may be appropriate in Azerbaijan. Regulators should also continue to promote professional development for bank personnel, since well-trained staff can ease bank-client interactions and indirectly advance regulatory objectives (because personnel are better able to implement and explain regulations).

To conclude, it can be said that even if the digital banking industry in Azerbaijan is on the rise and the overall performance is quite positive, there is still much to be done in terms of regulation. The next Chapter (Chapter IV) will consider the future of regulation, the issues to be solved, and the experience of regulating the market elsewhere. Basic analysis of this data will inform those conversations, and the issues and concerns raised by users (like what pieces of legislation need to be updated) will be addressed.

IV CHAPTER. FUTURE PROSPECTS OF REGULATION OF DIGITAL BANKING IN AZERBAIJAN

4.1. Analysis of the main problems in the regulation of digital banking in Azerbaijan

As noted above, the analysis conducted in Chapter III has disclosed the key problems associated with the regulation of the digital bank market in the Republic of Azerbaijan based on the results of the empirical survey and the special situation in the country, which in the future need to be addressed as a matter of priority.

Perhaps the biggest issue is that Azerbaijani legislation is unable to keep pace with the rapid development of electronic banking. This is supported by the results of the survey: close to half of the respondents considered legislation to be lagging behind progress in the banking sector (Q13) while a third of Q21 respondents chose legislative changes first on the list of needed improvements. For many years, laws and regulations on banking were generally applied to mobile applications, internet banking, e-wallets, and other digital banking services in Azerbaijan. However, there were no special laws on electronic money, fintech startups, open banking APIs, or other digital banking services. The new 2023 Law "On Payment Services and Payment Systems" partially covers some of these gaps (e.g., in the area of payment institutions and e-money institutions), but others are not addressed or are under-regulated:

• Open Banking and Fintech Integration: There remains no open-banking regime in place mandating banks to securely share customer data with third-party fintech providers like the European Union's PSD2 regime, potentially stifling innovation, and there are uncertainties about whether fintechs are allowed to serve as partners for banks.

• Digital identity and e-signatures: Digital identities/e-signatures are legally recognized in Azerbaijan. The lack of regulation may mean that digital identities/e-signatures are not fully interoperable and accepted between banks, requiring customers to create a new digital identity for each usage.

• Consumer protection issues in the digital world: Regulation may be avoided or remain silent on liability in the case of financial fraud, the procedures for handling mistakes, chargebacks in digital payments, etc. Banks may have their own rules, but there is uncertainty about what rights an user has in such cases. The main issue (Q10: 43% think rights are weak or not enough)

• Data Privacy: Azerbaijan has a Law on Personal Data. However, guidance on enforcement and case-specific rules should be further specified for financial services. Data protection is rated moderate given the rate of digital banking growth and the potential of the law to address such issues as data breaches and encryption in greater detail.

To summarize this, legislation is a problem in that it is not fit for the digital age, as one participant put it in M1Q21: "Müvafiq qanunvericiliyin yenilənməsi" (updating relevant legislation) is important. Otherwise, both the regulators and banks are not aware of what these new products are, and customers are not protected. All the other improvements are only peripheral without modern and strong legislation, which provides a foundation for everything else.

The lack of transparency was again highlighted in the survey. An important number of users believe that the actions of the regulators (Central Bank or the Financial Market Supervisory Authority, when it existed) are not transparent enough. Lack of transparency manifests itself in several ways:

• Opaque decision-making: The Central Bank's reasoning may not be publicly explained to the banks and the public in cases where it chooses to issue rules or make supervisory assessments behind closed doors. This may lead to uncertainty or even the impression that the Bank is favoring certain institutions. Since only 7.6% said they were "fully transparent", they may feel they do not have all the information they need.

• No Regular Publication of Findings: Audit findings, enforcement actions, or risk reports may not be regularly published. In some countries, regulators do publish the annual reports of the state of the banking system and consumer complaints and

resolutions. Such communications may, however, be scant or inconvenient in Azerbaijan.

• User Awareness of Regulations: Transparency of the regulatory process is not enough. Are users aware of the regulations that protect them? A large proportion of the respondents pointed to the need for "maarifləndirmə kampaniyaları" ("information campaigns"), which indicates that people are not sufficiently informed about digital banking protection programs and measures. Do people know what to do if their mobile banking app gets hacked, for example? Do they know the role of the Central Bank in this? If they don't, regulators have failed.

Lack of transparency: leads to distrust (because people trust things they know); rumor, anxiety and speculation (because the absence of information leads people to speculate and turn to rumors); and non-compliance (banks or users are not fully aware of rules and therefore may violate them). Better transparency delivers better communication, such as drafting regulation subject to public comment, announcing it in plain language, and publicizing regulatory oversight.

Another closely related issue is enforcing existing rules (and any rules that may be made in the future). Users said that regulators needed to monitor them closely (21.2% in Q21 picked this option). The chief problems here are:

• Possible Non-Compliance: Understanding that more than 71% believe banks do comply, almost 3 out of 10 disagree, suggesting that banks do not always comply or have taken more time to comply. For example, if the Central Bank declares a security standard, if some banks take time to conform, the central bank may need to follow up.

• Limited supervisory capacity: The regulator in Azerbaijan may be too small to monitor banks' IT infrastructure and cybersecurity using an adequate number of skilled IT auditors and SupTech as mentioned above. If the supervisor is understaffed and does not have access to modern analysis techniques, it may place too much trust in information provided by banks. The support for additional oversight suggests that users might believe (or fear) that the regulators do not always have a handle on what banks do digitally.

• Digital risk accountability: In the event of a major failure or breach in digital banking services, do the banks face penalties or meaningful consequences for failure to comply with their obligations for service continuity and protection against security risks? The lack of public enforcement actions may either mean that there are no violations (a positive outcome) or that violations are resolved in private, a problem of transparency and possibly moral hazard as banks may take risks thinking that their violations will go unpunished or unnoticed, which is not the case.

Essentially, however, the challenge is not updating the rules on paper, but in putting them into actual practice through enforcement. They want to see more proactive monitoring, on the spot testing of bank IT, regular stress testing of banks' digital systems, and fast remedial action. This is precisely the goal of the newly launched SupTech Roadmap [64], which seeks to use new technology for a risk-based approach to supervision. This is a process.

Issue (b) Although falling under the purview of law, we would like to highlight this issue because it may affect users' level of confidence. Only 11.9% of the respondents agreed that their rights are "fully protected". This points to:

• No User Rights Charter: User may not know if an unauthorized transaction occurs, the user has the right to a refund from the bank and the terms of that refund. While many jurisdictions have implemented such protections, like the EU (the EU Payment Services Directive states that unless user has been grossly negligent, banks must within reasonable time refund fraudulent transactions that are reported). However, if Azerbaijan does not have such a requirement, the policies of each individual bank prevail.

• Dispute resolution issues: If a customer has a problem with a digital service (wrong charge, service unavailable and they are losing business) how easy is it to get it resolved? The regulatory problem might be in ensuring there is an independent financial ombudsman or effective complaints escalation. Users can complain to the Central Bank, though many are unaware of it and feel unprotected if they do not prefer this process.

• Privacy and Data Security Enforcement: Moderate confidence in data confidentiality, but this could easily become an issue if data is breached. Do banks have to disclose a breach in their security to customers? Penalties for banks that mismanage or fail to protect client data could be more commonplace. Stronger consumer protections in digital finance, like the EU's General Data Protection Regulation, could include fines for companies facing data leaks. There is no practice of enforcement of banking data protection in Azerbaijan.

Without strong consumer protection, people will perceive digital banking as riskier than cash or branch banking. And those perceptions clearly matter (as our results show, trust is vital). That means the regulatory regime must strengthen these mechanisms, perhaps through new regulation and perhaps through better enforcement of existing regulation.

Although users never mentioned it as a problem (possibly because they are less aware of the processes behind the service), cybersecurity is an important challenge for experts in regulating digital banks. Respondents' experiences indirectly point to this issue: 16.1% of respondents said they need to invest in security tech, while 26.3% reported tech issues frequently. So the regulatory problem is highly complex:

• Setting Security Standards: In the domain of cybersecurity, regulators would have to come up with standards (e.g., internationally accepted standards like ISO 27001, PCI DSS for payment cards, etc. or local standards for banks, etc.) otherwise banks would have differing requirements.

• Systemic Preparedness: Digital banking connects banks, payment systems, and telecom networks. An incident at one can have system-wide effects. The regulator needs to ensure the whole ecosystem is resilient with backup systems and contingency plans. Are there regulations saying that banks need to have disaster recovery of digital services? What happens if a large mobile banking app goes down for days?

• Coordination on threat intelligence. A financial authority or central bank may collect and share cyber threat information about banks; if this is weak in

Azerbaijan, a regulatory coordination gap arises as each bank emerges from attempting to fend for itself.

Such incidents may add to the global cyber threat and, if not managed proactively, may lead to further serious incidents (which would seriously weaken trust).

6. Limited competition and innovation due to regulation: another challenge, which the polls do not explicitly mention, is the possibility of too much or too little regulation being detrimental to innovation and competition in digital banking markets:

• Where only banks can offer digital payment services or there are large barriers to entry for fintech companies, the result is weak competition and low innovation. Fortunately, the new payment services law addresses this, opening the door to non-bank payment service providers. How is it being applied?

• If open banking is not required, consumers cannot easily use new financial applications that aggregate accounts, etc., meaning that Azerbaijani consumers and fintech firms are therefore at a disadvantage relative to those in other countries.

Competition was not explored by the user survey, although it may be an implicit issue as a conservative regulatory framework stops incumbents from being challenged and better services being provided. The evidence from around the world is that strong but flexible regulation promotes both safety and innovation in financial services. For example, regulatory sandboxes can allow fintechs to test ideas under less regulation while someone still oversees. This was not common historically in Azerbaijan, but the fintech industry has increasingly moved in this direction through the Fintech Association and the Baku Fintech Forum. [65]

In summary, the main regulatory problems are the law (policy) gaps and implementation gaps:

• Policy gap: rules like laws and guidelines need updates to adjust to new realities of digital banking.

• Second, the implementation gap: even where rules already exist, these should be enforced transparently and with a strong focus upon users (through protection, empowerment and awareness-raising around their rights).

Azerbaijan is definitely not unique in this respect. Other countries have also struggled for bringing their laws into line with technological developments. How they address these problems proactively and strategically is the difference. These issues will be discussed in section 4.2 with respect to possible future directions for the Azerbaijani context, followed by a discussion in section 4.3 of lessons to be learnt from other countries.

Identifying these challenges as being outdated legislation, lack of transparency and enforcement, limited consumer protection, weak cybersecurity measures and regulatory hindrances to innovation, would help ensure that policymakers and regulators in Azerbaijan can address each issue and guarantee a safe, secure, and innovative digital banking experience for consumers.

4.2. Directions for solving the problems facing digital banking management in Azerbaijan

The solutions for these challenges will be multidimensional. This chapter concretely steps out and recommends actions that will improve the regulating and managing of digital banking in Azerbaijan. Following these survey results (what users themselves prioritized) and best practice, the recommendations should also be designed for the Azerbaijan context and take into consideration the country's legal system, capacities of institutions and market realities.

• Update Existing Laws: The Banking Law and other laws relating to financial services should be amended to expressly apply to electronic banking services. For example, all electronic contracts, communications and transactions in the banking sector must be as legally valid as those on paper. There should further be an express attribution of liability to online transactions. Definitions of terms such as "digital bank" or "virtual branch" in legislation should be kept up-to-date. Azerbaijan can create a working group consisting of representatives of the Central Bank, parliament

and the private sector to develop amendments to the legislation that will reflect new technologies and international standards. A change in banking practices (e.g. forcing banks to allow third-party payment initiators and data sharing in a secure way) could spur fintech innovation.

• Introduce New Regulations Where Needed: If there are completely uncovered areas, new regulations or secondary legislation will be introduced covering those.

- Open Banking Regulation: Regulate consent and bank data access by licensed third-party service providers, requiring rules on APIs, data privacy, liability distribution, and more. This would drive competition and transparency in banking as an industry problem, even forcing fintech innovation to occur under a regulatory umbrella, as it should be.

- Digital Onboarding/KYC: Regulations must allow banks to onboard customers completely through digital means and eKYC, with basic anti money laundering (AML) controls. This would enable digital banks to scale, as it is not feasible to have a physical presence of the bank in many cases.

- E-Money and crypto-assets: Building upon the new payment law establishing a legal framework for e-money, the Central Bank could issue additional regulations for e-money issuers (e.g. minimum capital, consumer protection standards, etc.) and develop a regulatory framework for crypto exchanges/stablecoins interacting with banks, though the latter is somewhat outside the banking sector. This would improve clarity and reduce risks.

- Implement a "Customers' Digital Banking Bill of Rights" regulation spelling out, for example, a right to timely error resolution; a right to privacy; a right to opt-out of information sharing; reasonable limitations on liability for unauthorized transactions (if reported in a timely manner); etc. This effort could be supplemented by a proper marketing campaign identifying customers' rights.

• Public Consultation and Expertise: Banks and fintech companies can provide feedback about operational feasibility. In addition, consumer advocacy is a nascent field in Azerbaijan. Organizations such as the Azerbaijan Consumers Union may be

able to provide input on consumer interests in that nation. International organizations like the World Bank and EBRD can be valuable partners for they often help with financial law reform and can present best practices that can be adopted across jurisdictions. If at the front end you solve the number one user problem with legislation, everything else flows from that.

• Improve Communication Channels: The Central Bank of Azerbaijan (CBA) and any other financial regulators should communicate more to the public. This could include:

- Regular press releases and reports on regulations: Press statements on new regulations and large decisions (e.g. fines on banks, introduction of new security requirements) and other technical terms could be issued in plain Azerbaijani and, possibly, in English explaining the implications for consumers. Digital banking reports on usage statistics, key risks, and regulatory actions could be posted on CBA's website once a year.

- Consumer-friendly guides. Simple guides or infographics explaining consumers' rights in digital banking and how to protect themselves. For example, a brochure or web-page: "Your rights in digital banking - what to expect from your bank and regulator", and what to do if something goes wrong. These should be broadcast through bank branches, websites and social media.

- Interactive Platforms: Social media or an online platform could be used to answer frequently asked questions and the regulator could for example host quarterly open online sessions, where users could ask questions and raise concerns. This would demystify the role of the regulator for transparency promotion.

• Regulation with a Consultative Approach: Seek feedback on draft regulations to increase transparency. Likewise, the regulator could distribute drafts of major digital banking rules and get input from banks, fintechs, and the public before finalizing the rules. Many jurisdictions do this to help build trust. The regulator will consider industry views. The regulator will consider consumer views.

• Transparency with enforcement: All supervisory actions can't be public (some can't be) but there are still ways to increase supervisor transparency. E.g. "The

Central Bank conducted an IT security assessment across banks and found X% compliance with standard Y; banks have been instructed to fix deficiencies by Z date." A bank's fine for a data breach, or failure to meet service availability commitments, should be public (at least in aggregate or anonymized form) to show rules are enforced.

• Education Campaigns. In relation to user understanding, respondents suggest the use of, for instance, short TV or radio advertisements providing general information about digital banking, working with universities to add topics on fintech and regulations to their offerings, or using the Fintech Association to present webinars to the public. Consumers with information are less likely to suffer fraud like phishing attacks. They also pressure banks and regulators for standards. These standards improve consumer fraud protections.

• Build Capacity for Digital Oversight: Regulatory bodies should ensure they can oversee and supervise digital banks effectively. This may require hiring or training additional IT auditors, cybersecurity specialists, and data analysts inside the Central Bank or Financial Supervision Authority. SupTech Roadmap (as discussed in media [64]), including use of advanced analytics to identify outliers (e.g. spike in failed transactions may be indicative of issues in the payment system or a cyber attack), machine learning to identify trends in the enormous quantity of data collected from banks (e.g. incident reports, downtime, complaints) and dashboard to monitor critical payment systems in real-time.

• Conduct Regular Audits and Stress Tests: All banks should undergo periodic digital risk audits. This can check compliance with security requirements, sufficiency of IT infrastructure, quality of data protection measures etc. The regulator can do these jointly with independent experts. Additionally, the regulator can run cybersecurity stress tests by simulating cyber incidents or big traffic spikes to see if banks can withstand them. Some of the major central banks have conducted such exercises (sometimes called "cyber war games") across the financial sector, with remedial actions for banks required.

• Known penalties and incentives about not following the regulations. Enforcing regulations is easier for authorities if people know what will happen if they don't comply with the rules. There should be known penalties for banks failing to report incidents or failing to achieve the new standard by the due date. Alternatively, there could be recognition for those banks that are setting the standard for best-practice (e.g., awards, public recognition), so the banks see the costs of compliance as a reputational benefit, not a cost.

Independent Oversight for Consumer Complaints: The financial ombudsman should be mandated or given a consumer protection unit with powers to investigate and adjudicate on consumer complaints that a bank is unable to resolve. Users should always have the option of raising a complaint with an independent body. If a third party is deemed strong and independent, consumers will feel more secure that where their bank fails, the system will not. Banks feel pressure to act responsibly. A third party can clean up, so banks know this.

• Regulators should watch for emerging risks in these areas for instance the public uses cryptocurrency in daily payments, new fintech apps emerge, and big tech may move into financial services, and consider what guidance and standards may be needed.

• Make "Digital Banking Customer Protection Regulation" law. Define customer and Bank liability for digital/online banking transactions performed without the customer's permission, and limit the customer's liability to the value of a transaction, e.g. 50□, to protect consumers. If a customer notifies the bank within 24 hours, then only the first transaction is lost. Otherwise, the customer loses, which spurs banks to invest in security capabilities and customers to report. Mandate maximum resolution time for fraud cases (e.g. banks to resolve any reported digital transaction dispute within 15 business days or provide a provisional credit). This gives consumers confidence in using digital channels.

• Data protection and privacy: Ultimately responsible for the banks' compliance with personal data rules, in coordination with the national data protection authority when one exists. More granular, perhaps adopting a small set of

the GDPR rules: data breach notifications to affected users within a specified time-frame, privacy impact assessments on new digital products, etc. As customers give banks a lot of personally identifiable information via their banking apps, banks need to take custodianship seriously. More than half of users believe their data is safe, and this must not only be maintained but increased. A single major data leak will destroy that confidence. Prevention and preparation are key.

• Insurance or Guarantee Schemes: The losses from cybercrime may be covered by some form of deposit insurance. Azerbaijan, for example, has a fund to cover losses from bank failures. What happens if somebody's bank account is hacked? Perhaps we can encourage or require that banks insure against such cyber-theft for their customers. This may be somewhat of a market solution (i.e. banks provide guarantee policies) but regulators can help encourage such policies by making it clear that saying "not our fault" in the case of a cyber incident is not enough in the absence of gross negligence by user.

• Focus on Inclusion: Digital finance regulation should ensure digital banking services grow and remain available for all. For example, regulators could ask from banks to offer all customers a basic digital account with a low fee or to make banking apps accessible for people with disabilities. Low financial literacy and financial inclusion (per Fintech Times) [65] are likely other important challenges, even if they were not highlighted by most in our survey results. While we are solving regulatory difficulties, we must not disproportionately disadvantage underserved communities. For example, when rules are made, should small banks be treated the same as big banks, and urban consumers be treated the same as rural consumers.

• Bank/fintech Financial-CERT: Form a Financial-CERT (Computer Emergency Response Team) in the banking/fintech sector under the guidance of the Central Bank to coordinate a cyber response between financial institutions, share threat and intelligence information, and conduct cyber drills. All banks should be obliged to participate, and with tech problems being raised by users, and increasing cyber attacks, a centralized body is the most efficient means of minimizing the damage done. The regulator can require banks to adopt certain IT security standards

like mandating multi-factor authentication on all digital banking logins that, although many banks have voluntarily adopted them, are more effective when enforced.

• Regulators may impose requirements for redundancy of digital banking infrastructure. Should one data center fail, systems will proceed uninterrupted and the data center will be backed up. And maybe even inter-bank backup for certain services (e.g. if one internet banking goes down, payments can still be routed via alternate networks). These are technical directions for enabling services to keep functioning even when the local infrastructure fails, protecting users from systemic downtime.

• Quality of Service Standards: The creation of minimum service level standards for digital channels (for example, a maximum percentage of downtime or total downtime in a quarter). Failure to meet these standards could trigger regulatory intervention. This is related to user experience. If banks must invest in IT (as regulations encourage), the risk technical issues pose to consumers becomes reduced. Even if no explicit regulation in these countries exists, as digital channels have only been growing in prominence, Azerbaijan could step ahead of the rest of the region by securing the availability of digital banking like a utility.

• Encourage innovation safely: On the issue of avoiding over-regulation, regulators should encourage banks and other players to push themselves on security, such as with biometric authentication and AI-based fraud detection. One way of doing this is with "innovation-friendly regulation". This has been used in a number of jurisdictions, such as the UK and Singapore, to describe the use of a regulatory sandbox to allow a bank, or other start-ups to test a new digital financial product, in a safe space, on a temporal basis. The concept is not a remedy to existing problems. Instead, it is a statement to the market that the regulators will not be hostile to that innovation and will help to attract fintech businesses to the country while showing that they will be open but careful with their scrutiny.

• Regulator-Industry Dialogue: Set up a Digital Banking Regulation Council or Committee which brings together regulators, banks and fintechs for regular discussions on emerging issues (e.g. a spike in a certain type of fraud, or new technology like digital IDs) so solutions can be co-created. This function improves compliance because banks have the opportunity to be heard and regulators are informed promptly. The Azerbaijan Fintech Association (AzFina) helps the public and private sectors interact in such arrangements.

• International collaboration: Given the global nature of threats and standards of digital banking, Azerbaijani financial regulators should increase cooperation with international organizations (IMF, World Bank, BIS... etc). Possibilities exist to adopt BCBS recommendations or guidelines on electronic banking risk management. Bilateral cooperation with neighboring countries such as Turkey and the CIS countries in the area of cybersecurity or payment systems integration may also indirectly improve regulation in these areas.

• Monitoring and revisiting reforms: Once new rules, practices or policies are introduced, regulators need to monitor the effects, and adapt them when necessary. If, say, a new rule places too many demands on banks and discourages them from providing a valuable service, the rule should be adjusted. When a problem arises, however, the rule is strengthened. The approach is one of slowly iterating, of solving problems with each iteration.

Some of these suggestions, including calls to reform laws, improve monitoring, invest in security, educate users and train staff, are directly discussed in comments 1, 2, 3, 5 and partly 4. The good news is that user perceptions appear to dovetail with legitimate and rational regulatory adjustments, which should be well-received.

• Some (like legal updates) require parliamentary action and political will.

• Others (such as other capacity building for internal regulators) need funding and training.

• Banks will also be responsible for upgrading their technology, training their staff, and cooperating with regulators.

• Crucially, the survey advocates for legislation and enforcement to be prioritized. So one sensible sequence might be: while waiting the next year or so for the key laws to be amended (perhaps the Central Bank can propose a Digital Finance Reform Bill containing many of the necessary amendments), increase transparency on initiatives in supervision (e.g. policies at the CBA), then consider the more technical and long-term reforms on matters such as cyber coordination, etc.

These and other measures might lead to improvements that will be picked up in future surveys so that over time, an increasing proportion of people will feel that their rights are being respected and that regulatory processes are open. Another possible measure is a reduction in the incidence or number of complaints about users experiencing technical incidents or resolving them more quickly.

However, it is not possible to remain inactive. Digital banking leaves no chance for delay and is developing rapidly, both globally and in the Republic of Azerbaijan. If these improvements to the regulatory environment are not made, Azerbaijan may be at risk from a future major fraud scandal or system crash. If they are made, however, a more enabling environment for digital finance in Azerbaijan may, alongside other policy measures, ease how the latter could contribute to economic growth through greater financial inclusion, productivity gains and the more efficient delivery of financial services.

Regulation will need to follow practical paths for (1) regulation and supervision, (2) innovation, and (3) education to address the challenges of digital banking. The above recommendations could be the roadmap for regulators. As Azerbaijan implements them, it can move towards a regulatory framework that is equally focused on fostering safety, trust and innovation, leaving the country's financial sector poised for strong digital growth.

4.3. Exploring the global experience of improving digital banking

There is experience that Azerbaijan can learn from elsewhere in dealing with the regulation of digital banking. Foreign regulators have struggled to some degree with the question of how to encourage innovation in the banking system while at the same time ensuring consumer protection and system stability. Various solutions have been suggested, so this section goes through relevant international experiences and their potential usefulness to what could work in Azerbaijan.

One of the most important legal reforms in digital banking is the European Union's Payment Services Directive 2 (PSD2). The PSD2, enacted in 2018, requires banks to open their payment services to third-party fintech firms via secure application programming interfaces (APIs) with customer consent. The PSD2's purpose was to stimulate competition and innovation by allowing fintechs to build on bank data or initiate payments, while also providing a high level of consumer protection, including requiring Strong Customer Authentication. In Europe it led to a large expansion in the number of non-bank services in particular (budgeting apps, multi-bank aggregators, etc.) as well as a large improvement in the convenience of them, while maintaining or improving the level of security (payment fraud rates have indeed decreased in many countries). Perhaps Azerbaijan has taken examples from this and seeks to roll out open banking principles in a similar fashion in order to create domestic fintech and improve consumer choice under a regulated framework. For example, your bank would be liable for your money if a payment through your account was made fraudulently, and you did not deliberately compromise any password. PSD2 establishes that, in such a case, the bank (or service provider) had to return your funds, usually within a day or two. These rules build trust.

The EU has passed the Digital Operational Resilience Act (DORA) legislation that sets rules for financial businesses to improve their cyber resilience and includes provisions such as regular cyber testing requirements, oversight of critical providers of financial services like cloud technology services, and incident reporting. Its provisions apply across the EU from 2025. These approaches show how other countries are taking an organized approach to cybersecurity as a regulation. In

Azerbaijan, a similar approach could be taken, compelling banks, as an example, to adopt best practice cybersecurity frameworks such as ISO and NIST.

Sandboxes have been introduced under UK, by the Financial Conduct Authority, and Singapore, by the Monetary Authority of Singapore, to support innovation while maintaining appropriate safeguards around risk. Sandboxes allow a fintech or bank to experiment with new digital products or business models with real consumers in a controlled environment under regulator supervision, with temporary relaxations of some regulations [66]. The FCA's sandbox, established in 2016, has been described as having helped the UK become a center for fintech as it has enabled faster introductions of new ideas such as app-only challenger banks and new payment solutions to the market, while helping the regulator learn about the innovations and providing guidance on compliance. Due to the small number of customers and/or transactions that can be involved in the sandbox, the impact of any failures is kept relatively small. Customers must also be compensated by the firms where necessary. In Singapore, sandboxes testbed the launch of blockchain-based payments and digital advisors. A sandbox would also send the signal that the country is open to fintech, attracting foreign investment and startups in the sector to Azerbaijan. The country also has a large amount of tech talent and an entrepreneurial youth that might otherwise go abroad or work in the grey economy. The sandbox allows the regulators in Azerbaijan to test and get used to new ideas. For example, a bank with no physical footprint and an entirely digital service may want to enter the market through a monitored launch rather than a conventional license. As global regulatory environments adapt quickly, jurisdictions using sandboxes will be in a better position to calibrate their regulatory and supervisory settings to effectively nurture digital banks. Azerbaijan is a low-risk candidate for such usage.

Some countries have gone further by providing special classes of licenses for banks that operate only online, sometimes called "challenger banks" or "neobanks".

• Hong Kong and South Korea have also issued licenses for virtual banks. Hong Kong licensed several virtual banks in 2019 with no physical presence

requirement, capital requirements, and cybersecurity standards. The new competition (higher deposit rates or new features to their apps) pressured incumbent banks to put more of their money into improvements while remaining supervised by the central bank.

• Malaysia and Singapore have also opened up applications for digital bank licenses, often with the aim of financial inclusion (to small-scale enterprises, the unbanked, the underbanked and the young) [66], with the licenses being given with the intent to achieve other policy objectives - in Malaysia, applicants were encouraged to fill gaps in existing banking.

The key regulatory understanding, here, is that flexible licensing is the best option, as, instead of a mandate that all institutions comply with the same regulatory requirements irrespective of their risk or business scale, regulators can impose requirements that are risk- and scale-appropriate. A branchless bank may have lower costs or dangers (like robbery/cash handling), but a higher risk elsewhere (like cyber). If it is not trading, the regulator could instead require different capital. It sets higher IT requirements assuming that the bank does not have a branch network to control. Azerbaijan may want to see how these banks evolve in other markets to determine whether, in a few years, a similar model would be appropriate for its local market, for niches the big banks do not serve. The timing of this road being followed would also depend on the ability to have that legal and supervisory capacity improved (see above).

In the US and Canada, regulatory and financial consumer protection agencies invest large efforts in financial literacy campaigns for digital finance products. For example, in the US, the CFPB publishes blog posts such as Protect yourself when banking online/mobile, and runs campaigns including Consumer Education Campaign on Identity Theft. Banks report to their regulator and educate consumers on apps and websites (e.g. reminding consumers that they should not share OTPs). It is generally agreed that an informed consumer base is the best deterrent against fraud and mis-selling. The experiences of several countries indicate that education should be continuous and should be adapted to the changing threat landscape. A few

years ago, phishing emails were an issue, now, it may be mobile app malware or social engineering. Azerbaijan could do this by establishing a consumer education unit within the Central Bank or the Ministry of Finance, and working with media and community organizations to promote financial literacy, particularly in digital finance. To do this, cooperation with international organizations such as the World Bank's financial capability programs could provide knowledge and financial assistance.

The EU's General Data Protection Regulation (GDPR) sets a high standard for data privacy law. It grants individuals a wide array of rights to control their data and imposes stiff penalties for misuse of data. GDPR applies to all sectors, but banks had to strengthen their practices in how they obtain permission, store data, and respond to customer requests to see or delete the data. The result is that, in Europe, consumers are better informed about the information collected by banks (thanks to more elaborate privacy notices) and are more able to refuse information sharing. A GDPR-style data breach notification requirement (where firms must notify the regulator and the user of serious breaches of data privacy within 72 hours) would also improve transparency. In Europe, direct notification from data controllers is required when data breaches are suspected to have occurred, and this greatly increases consumer trust. While Azerbaijan has its own data breach laws, more consistency with the GDPR would also substantially raise user trust. Transparency of consent and breach notification in financial services would be a good start. Data portability, as defined in the EU's GDPR, would allow consumers to ask for their data in a machine readable format to take to other financial services providers [67]. That idea, applied to banking (in the shape of the PSD2), drives competition and innovation, empowering consumers to use their own financial data to get better services.

Estonia is often used as an example of a digitalized society, including in the field of banking. An example of an improvement in digital banking services in the country was a unified digital identity infrastructure (e-ID), used by all banks in customer authentication. Led by the government, it greatly increases security and convenience, as customers only need one secure ID method to access any bank. This

lowers the risk of phishing (the customer does not store many passwords) and provides a high level of assurance (the ID is government-issued, and uses smart-card or mobile ID). Azerbaijan has Asan Imza (mobile ID), which could be further exploited as a main login for banking applications, like in Estonia. Estonia has a highly developed, close cooperation between its banks and government on cybersecurity, something that improved after the 2007 cyberattacks. Their model has been referenced to highlight the value of information sharing and public-private partnerships in securing digital finance. Many countries now operate Financial ISACs (Information Sharing and Analysis Centers) for threat intelligence sharing between banks and government. The establishment of the info-sharing group in the context of these sections 4.2 cyber recommendations is also in line with international practice as there are similar networks in the US (FS-ISAC) and Europe (coordinated via the ECB). The "we're all in this together" concept of defending against cyber risks would help improve resilience both at the individual level and for the system as a whole.

Another trend has been moving from rules to outcomes-based regulation of fintech. Australia's securities regulator issued a guideline on "RegTech". The guideline encouraged the use of AI to achieve compliance, and while it set out its regulatory expectations, also made clear it would accept compliance by alternative means if the desired outcome was achieved. In the banking domain, some authorities have started to signal that they are interested in outcome-based measures (low fraud rates, high availability, etc.) rather than prescriptions on how firms achieve them, leaving the details to the firms. Associated with this can be active supervisor-banker dialog on what exactly the banks are doing in this regard. For the developing regulators like Azerbaijan, an agile approach may be required. If a new mobile payment service is not clearly identifiable with one of the regulatory types, rather than banning or ignoring the new service, the Central Bank may wish to approve the service with conditions and monitor its behavior before amending the regulation. Internationally it is viewed as an experimental and safe way to prevent stifling on a promising new technology while managing the risks.

Globally, other nations have more concrete regulatory goals in mind, such as India's explicit regulations for digital banks, seeking to bring more people into the financial system. The Reserve Bank of India, India's banking regulator, licensed a new breed of bare-bones bank, called a "payments bank", which cannot lend, but can take deposits and offer payment services. It also introduced the unified payments interface (UPI). UPI will likely disrupt Indian retail payments. It's now an acronym that all banks and fintechs must get behind, and which the regulator will oversee. The result is a very competitive, innovative, stable, widely used and inclusive payment ecosystem. The main lesson for Azerbaijan is to clearly define what it wants from its digital banking market (greater uptake of cashless payments? Greater SME finance through digital platforms?) and regulate the market accordingly. If promoting financial inclusion is a goal, consider allowing non-bank players, such as postal networks or telecoms, under appropriate regulation to provide basic digital financial services in underserved areas. If promoting competition is a goal, guarantee non-discriminatory access to critical infrastructure (such as Payment systems and card networks) for new players, consistent with global best practice. If stability is the main concern for customer funds held digitally, prudential requirements could be placed on the holder, such as requiring e-money issuers to hold 100% reserves to protect consumers from firm failure.

As for these global practices, it is essential not to copy/paste them, but selectively use them and adapt them to the domestic context. The EU system is working well because of the existence of a developed legal order and a culture of data protection in the EU. A lighter responsibility in a smaller system may avoid overloading. Other principles may have universal benefits:

- Regulation which gives customers more control, information and protection is always a good thing, as it builds trust and enables digital banking adoption.
- Phased development (through sandboxes, pilot programs or phased licensing) can encourage innovation while allowing the financial sector to adapt without disruptions.

- Systemic resilience (through cybersecurity cooperation, operational standards, and testing) can prevent a crisis from pulling down the entire system.

Azerbaijan has a good chance of leapfrogging on some of the issues by learning through the experience of PSD2 and others, enabling it to form its open banking framework at a more advanced stage. This may include "open finance" going beyond data sharing between banks to the insurance and other sectors, which the EU has initiated following PSD2.

Finally, experience elsewhere is that continual adaptation is important and that digital banking will continue to evolve (think AI, digital currencies, etc). Internationally, regulators share experience (BIS, IMF, etc.) and Azerbaijan should continue to be plugged into these networks. The country is willing to learn and has worked on the SupTech roadmap together with the World Bank [64]. Other ways to ease keeping the regulatory framework modern could be to send staff abroad for training, to organize and attend fintech development conferences and to harmonize national laws with international standards (e.g. AML/CFT from the FATF, etc.).

Ultimately, Azerbaijan can avoid the pitfalls and learn from experiences globally, and has a menu of options. This menu includes for example the strong consumer and competition framework from the EU, the collaborative sandbox model of the UK, the licensing innovations in Asia and the leading experience of Estonia in digital security of online services. Coupling these with the local insights from our research (what Azerbaijani users and banks specifically need) will allow us to create a world-class, but home-grown regulatory environment. We envision a safe, transparent, and vibrant digital banking ecosystem in Azerbaijan that will thrive for many years to come.

CONCLUSION AND SUGGESTIONS

The aim of the study was to determine the regulation of the digital banking system in Azerbaijan and whether the users consider it effectively regulated. 118 users of digital banking systems were interviewed and statistical analysis was carried out in the SPSS program to identify the strengths and weaknesses of regulations.

The results show that the majority of Azerbaijani residents use digital banking apps, and find them useful for saving time and avoiding going to the bank. The data also shows that mobile devices are the most used online device, and that the public trusts the main banks, Kapital Bank, ABB and PASHA Bank. But many have experienced technical issues. Risk management in digital banking has been relatively successful, but there are legitimate concerns about the law, whether it is clear, and whether it is understood.

A regression analysis that looked for conditions under which people felt digital banking was secure found several factors. Banks must be regulated, and the laws must be revised to keep up with the changes in digital technology. If this is not the case, people are more likely to distrust the banks. People also said that they trust directly because regulation is strong, which means trust does not just exist in the background but functions and is important.

The study also found that users did not know the regulation, found it opaque, and wanted the provision of clearer rules, enforcement, and communication. They also want laws protecting their personal data. While people believe their data is protected, the majority are not certain.

The current legal framework does not yet cover new digital banking services. For example, open banking, online dispute resolution and new privacy laws are still underdeveloped. That creates confusion; and though the 2023 payment law is a step forward for users, they still see gaps.

Consequently, it has been recommended to take the following steps.

1. Update laws and regulations

The banking laws of Azerbaijan should contain specific provisions on digital banking services, electronic money, open banking and consumer protection in

banking, liability of payment service providers for unauthorized transactions, and the rights and obligations of banks providing online banking services. This is the first and foremost step.

2. Make regulation more transparent

Regulators should communicate new rules and regulations in plain English, more frequently and post user guides and financial reports about banks' compliance with regulations. Lots of communication leads to greater trust.

3. Strengthen monitoring and enforcement

For compliance, regulators must increase inspections, improve their own digital infrastructure, and penalize banks for any breaches. In digital banking, even very small failures can have big impacts so regulators must put preventative measures in place.

4. Improve consumer protection

Users should be informed about their rights and able to reach support when things go wrong. If the rules on refunds, complaints, and data protection are clear, along with a trusted dispute resolution system and a data protection authority, consumers will likely have more confidence when they use services.

5. Support cybersecurity and resilience

The use of common digital security standards among banks is recommended. The government can ease this by setting up a financial CERT to deal with digital security threats. If all banks follow good rules, and share warning signs, then big mistakes can be avoided.

6. Encourage safe innovation

Azerbaijan could introduce a regulatory sandbox which would allow digital products to be tried out under regulatory supervision and with guidance by the regulator. Special licenses for digital-only banks could help as well.

7. Learn from global experience

Countries such as the UK, Singapore and Estonia have successfully implemented differing defensive and offensive security strategies in the online

financial space that may be helpful for Azerbaijan. At the same time, changes should fit the context.

In summary, in addition to modern, transparent and protective regulation of digital banking services, there is a high degree of trust among Azerbaijanis towards the services used. However, potential future risks have not been left without concern. The government, regulators and banks must work toward creation of a safe, transparent and fair digital banking system. If someone acts before problems worsen and consumers lose trust regarding the system, Azerbaijan can lead in the field of digital finance in its region and provide its citizens safe and smart financial services.

REFERENCES

In English

1. Akhtar S., Ali K., & Alam N. (2018). “The potential of financial technology in East and North-East Asia.” United Nations Economic and Social Commission for Asia and the Pacific, 4p.

2. Allen, Hilary J. “Regulatory sandboxes.” George Washington Law Review, 87, 2019, p.580-645.

3. Artemenko D., & Bychkova I. “Legal framework for risk-based banking supervision in the digital age.” Financial Law Review, 2020, 19(3), p.81-102.

4. Ashta A., & Herrmann H. “The impact of digital transformation on banking, investments, and microfinance: Opportunities and risks.” Journal of Banking and Financial Innovation, 2021, 8(2), p.112-134.

5. Auer, Raphel (2019), “Embedded supervision: how to build regulation into decentalised finance.” BIS Working Paper, No 811, Bank for International Settlements, Basel, 31p.

6. Baba N., El Hamiani Khatat M., & Roulet C. “Fintech in Europe: Promises and threats.” IMF Working Papers, 2020, (59), p.1-36.

7. Bazarbash M. “Fintech in financial inclusion: Machine learning applications in assessing credit risk.” IMF Working Papers, 2019, (109), p.1-33.

8. Bazarbash M., & Beaton K. “ Financial inclusion and fintech: An analysis across countries.” IMF Working Papers, 2020, (150), p.1-28.

9. Boot, Arnoud et al. (2020), “Financial intermediation and technology: What’s old, what’s new?.” Working Paper Series, No 2438, European Central Bank, Frankfurt am Main, 34p.

10. Buchak G., Matvos G., Piskorski T., & Seru, A. “Fintech, regulatory arbitrage, and the rise of shadow banks.” Journal of Financial Economics, 2018, 130(3), p.453-483.

11. Cambridge Centre for Alternative Finance. (2024). “Global survey on fintech regulation: Trends and regulatory challenges.” Cambridge University Press.

12. Chomczyk Penedo A., & Trigo Kramcsák S. “Addressing bias in AI-based financial services through the European Financial Data Space.” Journal of Financial Technology and Regulation, 2023, 12(1), p.45-63.

13. Claessens S., Frost J., Turner G., & Zhu F. “Fintech credit markets around the world: Size, drivers, and policy issues.” BIS Quarterly Review, 2018(9), p.29-49.

14. Cohn T.H. “The Effects of Regulatory Capture on Banking Regulations: A Level-of-Analysis Approach.” The Failure of Financial Regulation: Why a Major Crisis Could Happen Again, 2019, p.71-110.

15. Cornelli G., Frost J., Gambacorta L., Rau P.R., Wardrop R., & Ziegler T. “Fintech and big tech credit: A new database.” BIS Working Papers, 2020, (887), p.1-45.

16. Crisanto J.C., & Ehrentraud J. “Big tech firms in finance: Regulatory challenges and policy approaches.” IMF Finance & Development Journal, 2021, 58(1), p.25-28.

17. Davis F.D. “Technology acceptance model: TAM.” Al-Suqri, MN, Al-Aufi, AS: Information Seeking Behavior and Technology Adoption, 1989, p.205-219.

18. Delle Foglie A., & Keshminder S. “Challenges and opportunities of SRI sukuk towards financial system sustainability: A bibliometric and systematic literature review.” Sustainability, 2021, 13(4), 1123p.

19. Dezem J., Oliveira D., & Fernandes L. “Open banking APIs: The balance between in-house and outsourced innovation.” Journal of Financial Innovation, 2023, 14(2), p.89-107.

20. Dwivedi Y.K., Rana N.P., Jeyaraj A., Clement M., & Williams M.D. “Reexamining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model.” Information Systems Frontiers, 2019, 21, p.719-734.

21. Eggert J. “A generic pattern matching approach for conceptual models in financial services: Assessing business process compliance.” Financial Computing and Regulation, 2021, 9(3), p.67-92.

22. Enria, Andrea (2022), “Interview with La Republica.” 18 May.

23. Frost J., Gambacorta L., Huang Y., Shin H.S., & Zbinden P. “BigTech and the changing structure of financial intermediation.” BIS Working Papers, 2019, (779), p.1-30.

24. Goetzmann, William N. (2016), “Money Changes Everything.” Princeton University Press, Princeton, NJ. 600p.

25. Gomber P., Kauffman R.J., Parker C., & Weber B.W. “On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services.” Journal of Management Information Systems, 2018, 35(1), p.220-265.

26. Gorton, Gary B. (2010), “Slapped by the Invisible Hand: The Panic of 2007.” Oxford University Press, New York, NY. 232p.

27. Hellwig, Martin “Systemic Risk in the Financial Sector: An Analysis of the Subprime-Mortgage Financial Crisis.” De Economist, 2009, 157, (2), p.129-207.

28. Herrera D., Pereira W., Volochen L., & Moreno A.M.Z. (2023). “Open Finance in Latin America and the Caribbean: Great Opportunities, Large Challenges.” IDB Monograph, NY, 95.

29. Huang Y., Wang H., & Zhang L. “The rise of big tech lending in China: Opportunities and challenges.” China Economic Review, 2020, 63, 101543p.

30. Infante J. “Central bank digital currencies and their macroeconomic implications. Journal of Economic Perspectives, 2021, 35(2), p.15-38.

31. Kapczynski, Amy “The Law of Informational Capitalism.” Yale Law Journal, 2020, 129, (5), p.1460-1515.

32. Kaur J., Sharma R., & Singh H. “Consumer perception towards risks in digital banking: A study in Northern India.” Journal of Banking and Technology, 2019, 10(1), p.45-67.

33. Laeven, Luc, Ratnovski, Lev and Tong, Hui, “Bank size, capital, and systemic risk: Some international evidence.” Journal of Banking & Finance, 2016, 69 (1), p.25-34.

34. Law S. “Virtual banks in Hong Kong: Regulatory challenges and financial inclusion.” Asian Journal of Financial Regulation, 2021, 6(2), p.78-95.

35. Lee J. “AI and digital banking: The role of machine learning and large language models in financial services.” Journal of Digital Banking, 2024, 11(1), p.22-39.

36. Mapuranga F. “Zimbabwe's fintech regulatory sandbox: Potential benefits and challenges.” Journal of African Financial Policy, 2024, 19(1), p.12-28.

37. Metrick, Andrew and Tarullo, Daniel K. (2021), “Congruent Financial Regulation.” BPEA Conference Drafts 25 March, The Brookings Institution, Washington, DC. 56p.

38. Najib M., & Fahma F. “Investigating the adoption of digital payment system through an extended technology acceptance model: An insight from the Indonesian small and medium enterprises.” International Journal on Advanced Science, Engineering and Information Technology, 2020, 10(4), p.1702-1708.

39. Navaretti G.B., Calzolari G., & Pozzolo A.F. “Fintech and banking: Friends or foes?.” European Economy – Banks, Regulation, and the Real Sector, 2017, (2), p.9-29.

40. Ofodile, B. O., Omankhanlen, A. E., Ibe, I. G., & Oaikhenan, H. E. (2021). Digital banking and regulatory frameworks: A comparative analysis between Nigeria and the United States. International Journal of Financial Research, 12(5), 66–76.

41. Pereira P. “Digital tokenization of non-financial assets: Legal challenges in English private law.” Journal of Law and Finance, 2023, 18(3), p.73-91.

42. Pflücke M. “Data access and automated decision-making in European financial law: Opportunities and risks.” Journal of European Financial Law, 2024, 15(1), p.42-58.

43. Philippon T. “The fintech opportunity.” NBER Working Papers, 2016, (22476), p.1-35.

44. Rau P.R. “Law, trust, and fintech platforms.” Journal of Financial Economics, 2020, 136(2), p.335-356.

45. Raza S.A., Umer A., & Shah N. “New determinants of ease of use and perceived usefulness for mobile banking adoption.” International Journal of Electronic Customer Relationship Management, 2017, 11(1), p.44-65.

46. Rogers E.M., Singhal A., & Quinlan M.M. “Diffusion of innovations.” In An integrated approach to communication theory and research, 2014, p.432-448.

47. Romano, Roberta (2018), “Pitfalls of Global Harmonization of Systemic Risk Regulation in a World of Financial Innovation.” in Amer, Douglas W. et al. (eds.) Systemic Risk in the Financial Sector: Ten Years After the Great Crash, CIGI Press, Waterloo, ON. 28p.

48. Shi W., Shambare N., & Wang J. “The adoption of internet banking: An institutional theory perspective.” Journal of Financial Services Marketing, 2008, 12(4), p.272-286.

49. Sinha A., & Roy S. “Comparative analysis of fintech growth and regulatory evolution in the US, UK, and India.” Journal of Fintech and Financial Policy, 2024, 20(1), p.30-52.

50. Suryono R.R., Budi I., & Purwandari B. (2020). “Challenges and trends of financial technology (Fintech): a systematic literature review.” Information, 11(12), 590.

51. Thakor A. “Fintech and banking: What do we know?.” Journal of Financial Intermediation, 2020, 41, p.100833.

52. Tio F., Sanjaya S., & Limantara N. “Analysis and Evaluation of User Interest Factors on Intention to Use Digital Bank.” In 2023 International Conference on Information Management and Technology (ICIMTech), 2023, p.357-361.

53. Truchet C. “Open finance: Opportunities, challenges, and policy implications.” Journal of Financial Innovation, 2024, 17(1), p.59-74.

54. Van der Boor, P., Oliveira, P., & Veloso, F. “Users as innovators in developing countries: The global sources of innovation and diffusion in mobile banking services.” Research Policy, 2014, 43(9), p.1594-1607.

55. Venkatesh V., Morris M.G., Davis G.B., & Davis F.D. “User acceptance of information technology: Toward a unified view.” MIS Quarterly, 2003, p.425-478.

56. Venkatesh V., Thong J.Y., & Xu X. “Consumer acceptance and use of information technology: extending the unified theory of acceptance and use of technology.” MIS Quarterly, 2012, p.157-178.

57. Vives X. “Digital disruption in banking.” Annual Review of Financial Economics, 2019, 11, p.243-272.

58. Wadesango N., Tinarwo R., & Wadesango V. “The impact of IFRS and IAS adoption on financial reporting quality.” International Journal of Accounting and Financial Reporting, 2021, 11(2), p.78-96.

59. Ziegler T., Shneor R., Garvey K., & Zhang B. “The global alternative finance market: Trends and regulatory developments.” Cambridge Centre for Alternative Finance Reports, 2020, p.1-56.

Internet resources

60. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2021:118:FIN

61. https://mspace.lib.umanitoba.ca/server/api/core/bitstreams/dbe8bbf4-7841-425a-9266-1c1932e57754/content

62. https://www.mondaq.com/financial-services/1451674/regulation-of-digital-payments-and-foreign-payment-systems

63. https://www.theeconomicsjournal.com/article/view/347/7-2-28

64. https://www.azernews.az/analysis/238042.html

65. https://thefintechtimes.com/richie-not-done-yet-fintech-in-the-caucasus-armenia-azerbaijan-georgia

66. https://www.mckinsey.com/industries/financial-services/our-insights/lessons-from-the-rapidly-evolving-regulation-of-digital-banking

67. https://www.researchgate.net/publication/367745236_DIGITAL_BANKING_AND_ITS_ESSENCE_THE_AZERBAIJANI_MODEL

APPENDIX

Survey questions

Demographic questions

Variable	Options
Gender	Male
	Female
Age	18–24
	25–34
	35–44
	45–54
	55 and above
Education level	Secondary education
	Vocational / college degree
	Bachelor’s degree
	Master’s degree
	Doctorate or higher
Primary bank whose digital services you mainly use	Kapital Bank
	ABB (International Bank of Azerbaijan)
	PASHA Bank
	Leobank
	Another local bank

Likert questions

(Scale: 1 – Strongly disagree, 2 – Disagree, 3 – Neutral, 4 – Agree, 5 – Strongly agree)

1. Regulatory framework and risk management	
I believe that in Azerbaijan the legal mechanisms for regulating digital banking are fully developed.	
I believe that the activities of regulatory bodies related to digital banking are sufficiently transparent for users.	
I think that the existing legislation in Azerbaijan keeps pace with the development speed of digital banking technologies.	
I believe that banks in Azerbaijan fully comply with the state's normative requirements regarding digital banking operations.	
I think that risk management mechanisms in digital banking are successfully implemented in practice.	
2. Technological, economic and trust-related factors	
I believe that technological security in digital banking systems is ensured at a sufficiently high level.	
I think that bank employees who work with digital banking services are specialized and adequately trained in this field.	
I believe that economic instability in the country negatively affects the regulation of digital banking.	
I think that customers' trust in digital banking directly depends on the level and quality of regulation.	
I believe that the personal data of individuals who use digital banking services in Azerbaijan are effectively protected by law.	