RISK MANAGEMENT IN THE REMOTE PROVISION OF BANKING SERVICES IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF BANKS

Zokir Mamadiyarov
Head of the Student Affairs Department, Ph.D, TSUE Tashkent 100047, Uzbekistan
z.mamadiyarov@tsue.uz

ABSTRACT

The rapid movement of information flows in the context of the COVID-19 pandemic is accelerating the FinTech revolution. In order not to lag behind in such conditions, banks need to gain customer confidence by studying customer demand, accelerating the remote organization of banking services, risk management in the remote organization of banking services, creating transparent and online platforms. After all, the introduction of modern FinTech products in the banking system will allow banks to attract customers, dramatically increase future revenues and reduce costs. In addition to the implementation of digital transformation of banks, the article presents the author's approaches to risk management and its impact on the existing ecosystem, the types of risks in the electronic banking system in recent years and these characteristics, as well as risk management related to remote banking services.

CCS CONCEPTS

• payment system; **• retail payment**; **• mobile banking**; **• electronic money**; **• risk**; **• cyber threat**; **• transformation. ACM Reference Format:**;

ACM Reference Format:
Zokir Mamadiyarov. 2021. RISK MANAGEMENT IN THE REMOTE PROVISION OF BANKING SERVICES IN THE CONDITIONS OF DIGITAL TRANSFORMATION OF BANKS. In *The 5th International Conference on Future Networks & Distributed Systems (ICFNDS 2021), December 15, 16, 2021, Dubai, United Arab Emirates.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3508072.3508119

1 INTRODUCTION

Today, digital technologies are rapidly entering all sectors of our economy. The development of e-commerce requires the formation and strengthening of a competitive environment between various payment service providers, the reduction of transaction costs for retail payments, as well as the introduction of innovative and attractive payment instruments that do not require the mediation of financial institutions.

Today, traditional banking services are being replaced by digital banking services. Because if banks do not improve the range of services, they may lose the opportunity to dramatically increase revenue and the number of customers.

The development of the financial services industry is accelerating. The FinTech trends we discussed above emerged in response to customer demand. They actually help providers provide better quality services that increase access to financial information, increase transparency, speed up transaction processing, provide remote services, secure methods of identification, and better support the customer life cycle.

In particular, the Decree of the President of the Republic of Uzbekistan dated May 12, 2020 No PF-5992 "On the Strategy of Banking Reform in the Republic of Uzbekistan for 2020-2025". as well as increasing the efficiency of the banking system through the gradual abolition of non-banking functions, complex transformation of state-owned commercial banks, introduction of modern banking standards, information technology and software products, widespread introduction of remote services for the population and small business, developing a network of low-cost service points. It is also planned to develop a strategy for reforming the banking system of the Republic of Uzbekistan for 2020-2025 to increase the popularity and quality of financial services by creating favorable conditions for the formation and development of non-bank credit institutions as a complementary part of the single financial system (Resolution, 2020).

Currently, the provision of banking services in developed countries is carried out remotely and online with extensive use of modern banking technologies. In the banking system of our country, the provision of banking services remotely and digital banking services is growing in line with modern requirements. For commercial banks, new banking products and services are an important tool in ensuring economic growth and competitiveness. However, despite the existing opportunities, the fact that the share of customers using the remote services of banks on average is 15-18% means that there are a number of problems in the development of the industry.

In particular, the digitization and remote organization of banking services leads to various risks associated with the implementation of services. Before managing these risks, it is necessary to eliminate such negative factors as the importance of remote banking services to customers, insufficient development of infrastructure in remote areas, lack of knowledge of the population in the field of remote banking services. Therefore, research to develop this area remains one of the most pressing issues today.

Digital transformation is one of the most important aspects in the provision of retail banking services in banks (2019). The rapid development of technology in the last few decades has changed the way people live and do business (Sardana, & Singhania, 2018).

ICFNDS 2021, December 15, 16, 2021, Dubai, United Arab Emirates

ACM ISBN 978-1-4503-8734-7/21/12…$15.00
https://doi.org/10.1145/3508072.3508119

Therefore, terms such as internet banking, online banking and e-banking have become widespread. The payment system has grown steadily over the past decade. The volume of global digital payments in the payment system is expected to reach $ 3,885.57 billion in 2019 and $ 8,686.68 billion by 2025 (Digital Payments Market: 2021).

The development of the Internet and mobile phones and their advantages in the economy have led to a radical change in the banking and financial system. Consumers who started using digital media to share data are now using company communication, online shopping, and many other new internet services (Alalwan et al., 2018; Alalwan et al., 2018; Cuesta et al., 2015; Rana et al., 2015).

Despite the development of remote banking services in Uzbekistan, during the COVID-19 pandemic, commercial banks faced many problems in the remote organization of banking services to the population and could not provide all services to customers remotely. It is obvious that remote banking services in Uzbekistan are not yet well established (Mamadiyarov, 2021).

The paper is organized as follows: Section I presents the relevance and relevance of the article today. In Section II, we present a review of relevant research on the topic. Section III describes the types of risks in the provision of banking services and their characteristics and methodological basis. Section IV develops proposals to address the problems of remote banking services. I conclude my paper in section V.

2 ANALYSIS OF THE RELEVANT LITERATURE

The introduction and use of information and communication technologies in banking will serve to increase the popularity of banking services. According to an infographic survey by Juniper Research, the number of users of digital banking and remote banking services in the world will reach 2.4 billion by 2020 and will increase by 54% to 3.6 billion by 2024. In 2019, banks have invested heavily in digital transformation and innovation. According to Juniper Research's Digital Transformation in Banking Readiness Index, although the scale of funding for digital transformation and innovation varies, Bank of America, BBVA and JPMorgan Chase are among the top three banks in terms of funding for digital transformation and innovation. Bank of America Erica has offered a wide range of digital solutions based on intuition in the use of chatbot and digital technologies, while BBVA Bank has focused on investing in APIs in the bank by offering a banking service platform, the BBVA Open Platform. JPMorgan Chase has experimented with blockchain (2020). Therefore, in most countries of the world, effective management of banking services and remote digital technologies without visiting the bank remains one of the most important tasks today.

Lewis Cohen, an associate professor at Cardiff University, studied the impact of risk on the desire to use remote banking services and found a positive correlation between desire and risk (Koenig-Lewis et al., 2010). It is important for people to consider the risk factor when using new technologies (Laforet & Li, 2005). The risk factor is very important when using remote banking services, as there is more risk than other offline services due to the remote online connection to bank accounts. L. Vessels and J. Drennan, on the other hand, studied the factors influencing the use of remote banking services and concluded that the risk had a negative impact on the use of these services (Wessels & Drennan, 2010). That is, the higher the risk when using new technologies, the more negative the impact on user choice (Mamadiyarov, 2021).

Security risk is the possible loss due to fraud or hackers 'intrusion into the security of e-banking. Since the 1960s, the concept of risk theory, adopted to explain consumer behavior in research, has been introduced into science. "Risk is defined as the subjective determination by a user of an online bank of losses in their online activities," he said (Lee, 2009).

Featherman and Pavlow described risk as the "probability of loss in pursuit" of any outcome of using an e-service (Featherman & Pavlou, 2003). The more money customers have involved in a transaction, the greater the risk. In this case, they increase the risk they anticipate and reduce confidence in e-banking (Yang et al., 2015). In addition, the intention to use online banking is mainly negatively affected by security risk and financial risk.

As a result of the development of information technology and the Internet, banks are changing the way they offer and use modern financial services, especially mobile internet and mobile technology (Bhatiasevi, 2016; Laukkanen, 2016; Oliveira et al., 2014). We can highlight mobile banking services in the set of communication channels to the new bank provided by banks (Mohammadi, 2015).

Innovative solutions in the development of the economy create competition for banks, for example, the improvement of mobile banking services can contribute to the simplification of financial services (COLE et al., 2011). In addition, this technology can be effective in providing a wide range of financial services (Gurgand et al., 1996).

However, one of the obstacles in introducing new technologies to the banking system is its purchase, and the other is the cost of using it. It was found that the high cost of using them also has a negative impact on the development of remote banking services. On the other hand, low prices encourage customers to use remote banking services (Sathye, 1999).

3 TYPES OF RISK AND METHODOLOGY

Adoption of the Law of the Republic of Uzbekistan "On Payments and Payment Systems" has created a legal basis for the circulation of electronic money, including the issuance, use and redemption of electronic money.

On the basis of this law, "Rules for the issuance and circulation of electronic money in the territory of the Republic of Uzbekistan" was developed and registered in the Ministry of Justice on April 29, 2020 No 3231.

This document is based on world experience and is designed to organize the activities of the electronic money system, the circulation of electronic money, risk management in the electronic money system and security in the system.

Accordingly, the issuer, the operator, the agent of the electronic money system, the owner of the electronic money, as well as banks, payment organizations, individual entrepreneurs and (or) legal entities that have entered into an agreement with the issuer are the subjects of the electronic money system (Figure 1). In this case, the bank that provides the operation of the electronic money system and (or) a payment organization with the appropriate license - is the operator of the electronic money system. An issuer or other

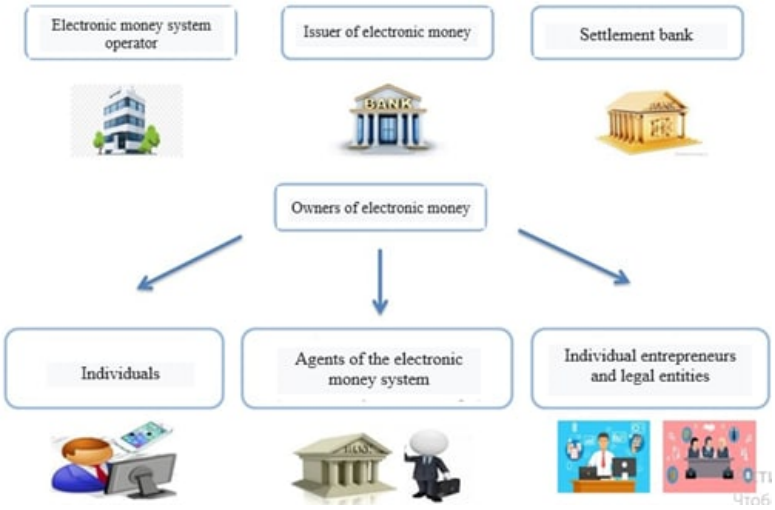

Figure 1: Subjects of electronic money system (Source: https://cbu.uz/oz/press_center/news/268736/)

non-issuer bank may act as a settlement bank of the electronic money system on the basis of an agreement with the operator.

It should be noted that in order to start its activities, the issuer must first send to the Central Bank a notice in the prescribed form on the issuance and sale of electronic money and attached to it samples of contracts with the operator and contracts with electronic money.

This normative-legal document stipulates that transactions in the electronic money system must be carried out by the operator in accordance with the rules of the electronic money system. These rules are approved on the basis of an agreement between the operator and the issuer. In a multi-issuer electronic money system, these rules must be agreed with each issuer.

The issuer and the operator of the Republic of Uzbekistan "On Combating Money Laundering, Terrorism Financing and Financing of Proliferation of Weapons" takes measures to ensure and implement organizational and procedural measures in accordance with the requirements of the Law.

Detection of fraud in the electronic money system of the issuer and the operator, as well as the financing of money laundering, terrorist financing and proliferation of weapons of mass destruction. In order to prevent them, it will take measures to ensure and implement organizational and procedural measures in accordance with the requirements of the Law of the Republic of Uzbekistan "On Combating Money Laundering, Financing of Terrorism and Financing the Proliferation of Weapons of Mass Destruction."

The electronic money system is protected from prohibited payments on the basis of the rules of use of the system and the agreements concluded between the subjects of the electronic money system.

At the same time, it is necessary to ensure the software and hardware of the electronic money system and the means and measures to prevent unauthorized access to electronic wallets, as well as organizational measures to ensure adequate protection of information.

Procedures for information security and protection used in the electronic money system must ensure continuous protection of information at all stages of electronic money circulation, including:

- determination of the rights of the owner of electronic money to carry out transactions with electronic money;
- to determine the causes of incidents detected in transactions with electronic money;
- protection of information from unauthorized access and ensuring the integrity of information.

In accordance with the agreement between the issuer and the operator, the issuer or operator maintains an account of information on the balance of electronic money in the electronic wallets of electronic money holders and the operations performed by them.

The operator ensures the registration of all transactions made using electronic wallets, the formation of statistical and informational reports on transactions and storage of transaction information in the format in which they were formed, sent or received, for at least five years, subject to integrity and immutability.

Risk management in the electronic money system should be based on the following:

- storage of information on internal control and audit procedures of the system, system operation and transactions;
- information system that provides timely processing, accounting and storage of information on each transaction, protection and storage of data in the system;
- availability of qualified staff (Resolution, 2020).

The most dangerous thing in the process of digitization of the banking system, storage of funds in numbers and the implementation of the payment system online is the presence of very high risks associated with them.

The UK's TESCO Bank said it was experiencing frequent fraudulent transactions among its nearly 40,000 customers and immediately shut down its online payment system. The bank's executive director said the bank had been subjected to a "systemic complex

Figure 2: The most common types of cyber threats to banks and customers (Source: https://cybersecure.uk.com/biggest-risks-of-online-banking-and-how-to-avoid-them/ compiled by the author based on the data.)

attack", which we knew for sure, but could not disclose further because it was part of an investigation (Nikolov, 2021).

Here are the most common cyber threats to bank customers and banks themselves:

- open mobile banking applications;
- aggressive banking malware;
- unstoppable DDoS attacks.

Open mobile banking applications. In 2015, nearly 70 percent of the top 100 mobile banking apps running on the Android app were well-established for security and data breaches. However, in some cases, security vulnerabilities would be visible, such as intentional cheating, data spread to an unknown address, SQL injection, JavaScript injection, and XML injection, among others.

Fortunately, most banks have implemented additional security measures, such as two-factor authentication using electronic tokens, one-time passwords, and security codes sent to Android phones. Nevertheless, cybercriminals have developed tools and malware capable of bypassing these security measures.

Aggressive banking malware. Dridex, Dyre, TrickBot, and Lurk - these are the most common trojan programs used to access online account records and steal data.

Dyre, one of the most dangerous Trojan viruses created for the financial market, has caused hundreds of millions of dollars in damage by manipulating websites to disrupt communication between more than 400 financial institutions and their clients. Many banks, such as the Royal Bank of Scotland, Bank of America and JP Morgan Chase, have become its “victims”.

This malware works by installing it on the user’s computer and is activated when the user enters trust credentials on a specific site, usually a banking institution or financial service login page. Through an Internet browser, hackers can steal account information and use their accounts for other purposes. Of course, all this is done in complete secrecy. In particular, in 2016, the Lurk Banker Trojan targeted several Russian banks via e-mail and stole $ 25 million from customers ’accounts.

TrickBot is one of a new type of software that has caused a lot of damage to Australian banks. It is very similar to Dyre, but according to IBM, in recent years there has been a program with "the most advanced browser techniques" among the malware of banks (Nikolov, 2021, November 9).

Unstoppable DDoS attacks. DDoS (distributed denial-of-service) attacks online systems such as internet banking sites or online trading platforms, which have a lot of data to overload them and cancel their services.

Studies show that DDoS attacks are one of the most serious security risks recognized by the banking industry. According to a 2015 report by U.S. wireless network operator Verizon Communications, they account for 32 percent of all attacks on banks. Not surprisingly, these tools are common on the internet. DDoS attacks are similar to the expected traffic from high levels, they get stuck on the highway, preventing constant traffic from reaching its destination.

This means that the activities of commercial banks are highly digital and require an assessment and effective management of the risks that may arise in the operation of online operations. The following are a number of types of risks that may arise as a result of the digitization of traditional banking activities as a result of the transformation of banking activities and increase the level of risk:

- operational risk;
- security risk;
- reputation risk;
- legal risk;
- risk of money laundering;
- cross-border risk;
- strategic risk;
- other traditional risks.

Operational risk. Operational risk or transactional risk is the most common type of risk in e-banking. These include:

- improper execution of transactions;
- violation of data integrity and disclosure of data confidentiality;
- unauthorized access to banking systems;
- non-performance of contracts, etc.

In addition to technological errors, human factors such as negligence (customers or employees), employee fraud, hackers, etc. are a potential source of e-banking operational risk.

Security risk. When it comes to banking operations, the security of the operation is paramount. All customers want their transactions to be confidential.

However, since all the information is on the internet, someone may get the information and misuse it. The security risk of

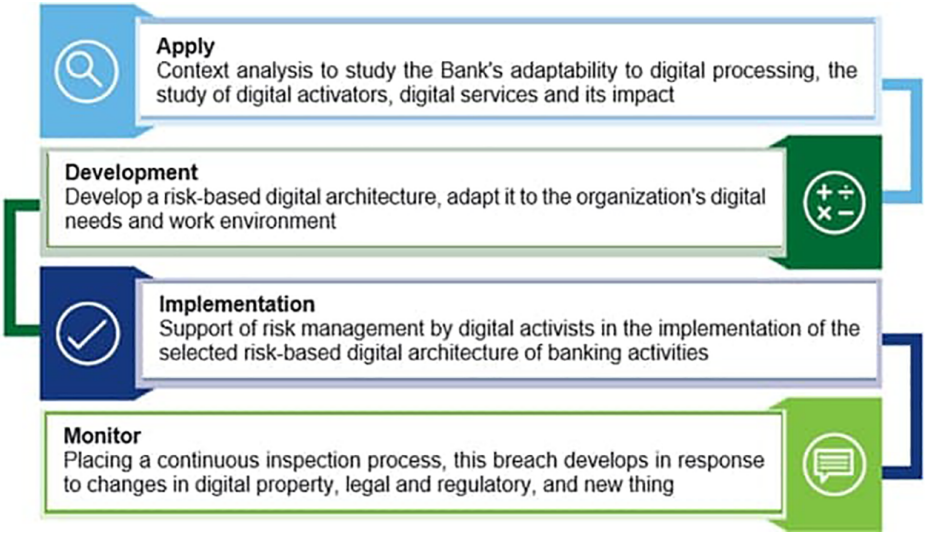

Figure 3: An approach to effective risk management in a digital environment

e-banking also stems from hacking threats and unauthorized access to banking systems.

It is important that the bank has the appropriate system architecture and management tools to manage the various operational and security risks of e-banking. If the bank has an outdated and non-renewable system, then it can become an investment loss for the bank, along with inefficient service.

Banks need to keep their systems up to date to keep up with fast-changing technologies to prevent loopholes in their security system. In addition, bank employees need to be regularly trained to keep abreast of new technologies.

Reputational risk. Its reputation is very important for any bank and other business as well. When it comes to digital banking, if a bank is unable to perform its functions or perform at the level of quality expected by its customers, then there is a risk of losing its reputation. This will eventually lead to the loss of funds or customers.

Some of these risks include system or product failure as expected, serious system failures, security breaches (external or internal), misinforming customers about e-banking processes and policies, some communication problems that prevent the customer from accessing his account, and more. possible.

Legal risk. If laws, rules, regulations, or established practices are violated, or if the legal rights and obligations of any of the parties to the transaction are not established, then these circumstances create a legal risk.

The e-banking system is a relatively new system, with some more uncertainty and controversy over some laws and regulations. This increases the legal risk. There is a lot of work to be done in Uzbekistan in this regard. Improving existing legislation and by-laws is a requirement of today.

The risk of legalizing crimes. All transactions are carried out remotely through electronic banking channels. Therefore, the use of traditional methods to detect and prevent criminal activity is not effective for banks.

While there are certain rules for the legalization of crimes, there are many aspects of electronic payments that are inconsistent and not covered in their implementation. Therefore, banks bear the risk of money laundering.

Cross-border risk. The main idea of e-banking is to expand the geographical capabilities of both the bank and its customers. This means that as a result of the expansion, it is possible to go beyond national borders. This leads to several cross-border risks:

- legal and regulatory risks - uncertainties about legal requirements in some countries and uncertainties in the jurisdiction of various local authorities;
- operational risk - if the bank uses a service provider located in another country, it will not be possible to monitor the process and will lead to operational risk;
- credit risk - Cross-border transactions can increase credit risk. This is because it is difficult to evaluate an application for a loan from a client in another country and the paperwork is not uniform.

Strategic risk. This risk is related to the following issues:

- business plan development;
- have sufficient resources to support the business plan;
- reliability of partners in working with external partners;
- any change in the work environment for employees;
- he degree to which existing technologies compete with modern technologies.

Digital technologies are gradually being recognized as an important process activator. The digital transformation comes forward, creating opportunities for unequal value creation and growth. Therefore, innovative approaches are needed to conduct research and find solutions for effective risk management in the digital environment (Figure 3).

4 RESULTS

We provide recommendations on the risks, consequences of risks and how to overcome the challenges that digital transformation can create.

First, work with multicloud (multi-cloud) or hybrid cloud (hybrid cloud) infrastructures. Many organizations are moving from multiple providers to an IT environment supported by multi-cloud services. This may include software as a service (SaaS), platform as a service (PaaS), or infrastructure as a service (IaaS).

Regardless of the type of use of the cloud, the placement of important data and applications by financial institutions outside the protection layer poses an even greater risk, especially if they involve multiple locations, services, or partners. In addition to data loss or theft, banks and customers may face problems with data privacy rules, which puts them at risk of overhead costs due to poor cloud management practices.

Today, consumers and businesses are accustomed to doing their work quickly through social networks and e-commerce. They, in turn, expect similar fast-service products from banks.

Second, large competitive pressures, aggressive FinTechs (major FinTech firms competing with Square and PayPal banks), and some well-known non-bank credit institutions, i.e., automated processes and created risk management models. As a result, they have reduced service fee and pricing policies compared to traditional banks (studies have shown that digital banks expenditures accounted for 33 percent of revenues, while existing banks accounted for 55 percent).

Third, cost pressures come from a different direction, i.e., regulatory constraints and low interest rates have in many cases made the average return on capital lower or closer to the cost of capital. While these problems can be overcome, the pressure can remain, especially as banks have to hire more staff to manage risk and ensure compliance.

Fourth, as new banking models emerge and evolve, the types of risks are also being updated. For example, digital channels pose new types of risks (including greater exposure to digital assets). The growth of analytics requires risk managers to pay close attention to model risk, and the high level of interdependence between enterprises requires caution against infectious risk.

Fifth, the fact that many people admit that the regulation of banking activities has reached the level of "top regulation" surprised some experts. Thirty percent of those surveyed said the cost of risk management has increased by more than 50 percent over the past five years. In addition, 46 percent forecast that spending will continue to rise slightly over the next five years. Although some aspects are not somewhat regulated, a general increase in regulatory constraints on topics such as banking supervision (e.g., TRIM and SREP), systemic risk (e.g., stress tests and Basel III), data protection (such as GDPR) can be expected.

Digitization can also be a powerful help in coping with the consequences - nearly 100 percent of respondents, regardless of geography or category (G-SIB and D-SIB), say digitization is an important tool to overcome the regulatory burden. Regulation, on the other hand, is not a major barrier to digitalizing risk. According to respondents, the most important barriers are old IT (85 percent), database problems (70 percent), culture (45 percent), lack of talent (40 percent), and complex organizational structures (40 percent).

Other risks of e-banking are the same as traditional banking risks, credit risk, liquidity risk, interest rate, market risk and so on. However, in the e-banking system, these risks can be characterized by the use of electronic channels and the fact that they are not geographically limited.

Some of the shortcomings that pose all of the above risks may be due to insufficient technology, staff negligence, and unauthorized access to the system. Therefore, it is important that banks adopt the right technologies and systems and create a secure operating environment.

The author conducted a survey on the development of remote banking services in Uzbekistan in 2020 and made an econometric analysis of the factors influencing the development. According to him, the system is convenient to use remote banking services, the security of personal data in remote banking services, the importance of remote banking services in saving costs and the quality and speed of the Internet in the implementation of remote banking services (Mamadiyarov, 2021).

5 CONCLUSION

In conclusion, the widespread introduction of new technologies in the banking and financial system of Uzbekistan has the following advantages:

- Increasing the number of bank customers - providing more people with banking services;
- Raising the status of private banks - reducing government funding;
- Shadow economy - it is possible to reduce the potential;
- Tax collection will be easier;
- Positive impact on production;
- Increased resilience to competition from global banks, etc.

Problems in cost, problems, and risk management in the FinTech industry include:

- it is necessary to create an infrastructure that can constantly collect information;
- create the ability to analyze too much information;
- adoption of new technology without full understanding of the risks;
- lack of knowledgeable professionals.

Further development of remote banking services provided by the banking system of Uzbekistan, identification of the population's demand for such products and services through marketing services and, consequently, changes in the banking strategy will ensure the bank's stability and competitiveness in this market segment.

REFERENCES

[1] Appendix to the Resolution of the Board of the Central Bank of the Republic of Uzbekistan No. 13/3 of February 15, 2020 "Rules of issuance and circulation of electronic money in the territory of the Republic of Uzbekistan"

[2] Mamadiyarov, Z. (2021). Analysis of factors affecting remote banking services in the process of bank transformation in Uzbekistan. Financial and Credit Activity: Problems of Theory and Practice, 1(36), 14–26. https://doi.org/10.18371/fcaptp.v1i36.227607

[3] PWC's Global Consumer Insights Survey 2019. Payments Cards & Mobile. (2019, April 18). Retrieved November 29, 2021, from https://www.paymentscardsandmobile.com/global-consumer-insights-survey-2019/.

[4] Sardana, V., & Singhania, S. (2018). Digital technology in the realm of banking: A review of literature. International Journal of Research in Finance and Management, 1(2): 28-32. https://www.allfinancejournal.com/article/view/12/1-2-8

[5] [Digital Payments Market: 2021 - 26: Industry share, size, growth - mordor intelligence. Digital Payments Market | 2021 - 26 | Industry Share, Size, Growth - Mordor Intelligence. (n.d.). Retrieved November 29, 2021, from https://mordorintelligence.com/industry-reports/digital-payments-market.

[6] Alalwan, A. A., Baabdullah, A. M., Rana, N. P., Tamilmani, K., & Dwivedi, Y. K. (2018). Examining adoption of mobile internet in Saudi Arabia: Extending Tam with perceived enjoyment, innovativeness and trust. Technology in Society, 55, 100–110. https://doi.org/10.1016/j.techsoc.2018.06.007

[7] Alalwan, A. A., Baabdullah, A. M., Rana, N. P., Tamilmani, K., & Dwivedi, Y. K. (2018). Examining adoption of mobile internet in Saudi Arabia: Extending Tam with perceived enjoyment, innovativeness and trust. Technology in Society, 55, 100–110. https://doi.org/10.1016/j.techsoc.2018.06.007

[8] Cuesta, C., Ruesta, M., Tuesta, D., & Urbiola, P. (2015). The digital transformation of the banking industry. BBVA Research Digital Economy Watch, https://www.bbvaresearch.com/wp-content/uploads/2015/08/EN_Observatorio_Banca_Digital_vf3.pdf (bbvaresearch.com)

[9] Rana, N. P., Dwivedi, Y. K., Lal, B., Williams, M. D., & Clement, M. (2015). Citizens' adoption of an electronic government system: Towards a unified view. Information Systems Frontiers, 19(3), 549–568. https://doi.org/10.1007/s10796-015-9613-y

[10] Juniper Research: Digital Banking users to exceed 3.6 billion globally by 2024, as digital-only banks catalyse market. Business Wire. (2020, March 3). Retrieved November 29, 2021, from https://www.businesswire.com/news/home/20200302005659/en/Juniper-Research-Digital-Banking-Users-to-Exceed-3.6-Billion-Globally-by-2024-as-Digital-Only-Banks-Catalyse-Market.

[11] Koenig-Lewis, N., Palmer, A., & Moll, A. (2010). Predicting young consumers' take up of Mobile Banking Services. International Journal of Bank Marketing, 28(5), 410–432. https://doi.org/10.1108/02652321011064917

[12] Laforet, S., & Li, X. (2005). Consumers' attitudes towards online and mobile banking in China. International Journal of Bank Marketing, 23(5), 362–380. https://doi.org/10.1108/02652320510629250

[13] [Wessels, L., & Drennan, J. (2010). An investigation of consumer acceptance of m-banking. International Journal of Bank Marketing, 28(7), 547–568. https://doi.org/10.1108/02652321011085194

[14] Lee, M.-C. (2009). Factors influencing the adoption of internet banking: An integration of Tam and TPB with perceived risk and perceived benefit. Electronic Commerce Research and Applications, 8(3), 130–141. https://doi.org/10.1016/j.elerap.2008.11.006

[15] Featherman, M. S., & Pavlou, P. A. (2003). Predicting e-services adoption: A perceived risk facets perspective. International Journal of Human-Computer Studies, 59(4), 451–474. https://doi.org/10.1016/s1071-5819(03)00111-3

[16] Yang, Q., Pang, C., Liu, L., Yen, D. C., & Michael Tarn, J. (2015). Exploring consumer perceived risk and trust for online payments: An empirical study in China's younger generation. Computers in Human Behavior, 50, 9–24. https://doi.org/10.1016/j.chb.2015.03.058

[17] Bhatiasevi, V. (2016). An extended UTAUT model to explain the adoption of mobile banking. Information Development, 32(4), 799–814. https://doi.org/10.1177/0266666915570764

[18] Laukkanen, T. (2016). Consumer adoption versus rejection decisions in seemingly similar service innovations: The case of the internet and mobile banking. Journal of Business Research, 69(7), 2432–2439. https://doi.org/10.1016/j.jbusres.2016.01.013

[19] Oliveira, T., Faria, M., Thomas, M. A., & Popovič, A. (2014). Extending the understanding of mobile banking adoption: When utaut meets TTF and ITM. International Journal of Information Management, 34(5), 689–703. https://doi.org/10.1016/j.ijinfomgt.2014.06.004

[20] Mohammadi, H. (2015). A study of mobile banking loyalty in Iran. Computers in Human

[21] COLE, S. H. A. W. N., SAMPSON, T. H. O. M. A. S., & ZIA, B. I. L. A. L. (2011). Prices or knowledge? what drives demand for financial services in emerging markets? The Journal of Finance, 66(6), 1933–1967. https://doi.org/10.1111/j.1540-6261.2011.01696.x

[22] Gurgand, M., Pederson, G., & Yaron, J. (1996). Rural finance institutions in Sub-Saharan Africa: Their outreach and sustainability. Savings and Development, 20(2), 133-168. https://www.jstor.org/stable/i25830571

[23] Sathye, M. (1999). Adoption of internet banking by Australian consumers: An empirical investigation. International Journal of Bank Marketing, 17(7), 324–334. https://doi.org/10.1108/02652329910305689

[24] Nikolov, I. (2021, November 9). Council post: Top Five cybersecurity threats and how to avoid them. Forbes. Retrieved November 29, 2021, from https://www.forbes.com/sites/forbestechcouncil/2021/11/09/top-five-cybersecurity-threats-and-how-to-avoid-them/.