# Accounting Aspects of the Risk of Digital Payment Operations in Bulgarian Banks

Rumyana Marinova - Chief Assist. Prof. PhD
University of Economics - Varna, Varna, Bulgaria
r_marinova@ue-varna.bg

**Abstract**

*Changing banking business models through the introduction of digital innovations is of key importance for the future development of the banking system, but at the same time it is related to the development of existing and new risks for banks. The purpose of this publication is to carry out a critical analysis of the risk of the introduction of various digital banking products and services in the field of payment operations and, on this basis, to outline the specific accounting aspects of this risk. Our conclusions are related to the understanding that the differentiated disclosure of incurred costs and/or reported losses from the occurrence of cyber risks in the financial statements of banks related to digital products and services and in particular to digital payment operations is necessary in order to correctly define, evaluate and analysis of those risks by all users of financial information.*

*Keywords: digital payments, operational risk, cyber risk, banks, IFRS*

*JEL Code:G20, M41*

## Introduction

Banks have grown very dynamically in recent years, and the challenges posed by the COVID-19 pandemic only increase the requirements for a new way of serving bank customers. It is an indisputable fact that digitization, the offer of adequate products and the possibility of remote access to the offered portfolio of services provides competitive advantages to those banks that manage to successfully implement them in their operations. The use of technology will increase, the structure of jobs will change as consumers increasingly demand to be served when and where it is most convenient for them. The mentioned facts brought out the digitization of banking activity as the main factor for achieving sustainable long-term growth, but at the same time, the issues related to the risks that digitalization brings are already on the agenda.

The aim of this publication is to carry out a critical analysis of the risk of the introduction of various digital banking products and services in the field of payment operations and, on this basis, to outline the specific accounting aspects of this risk.

The scope of the study includes the five largest Bulgarian banks based on their total assets, grouped by the Banking Supervision Department into the first group. The study covers publicly available information from the examined banks as of October 2022. The present research is limited to the examination of one aspect of the digitization of banking operations - the digitized payment services provided by banks to individual clients.

### 1. Digitization of banking products / services and related risks.

In the second quarter of 2022, according to data from the quarterly report of the Bulgarian National Bank, the banking sector operated in conditions of accelerated inflation and increased uncertainty in the economic environment. The report notes that risks to the environment have been exacerbated by significant increases in energy prices, potential disruptions in supply chains, and the prospect of a slowdown in external demand. (BNB, 2022)

At the same time, according to NSI data for 2021, in Bulgaria only 14.9% of the population using the Internet for personal purposes, actually uses Internet banking (including mobile banking). In 2020, this percentage was 12.6%, and for 2019 – only 8.6%. 83.5% of all households had access to the Internet in 2021. (НСИ, 2021) There is an increase, albeit a small one, in the number of people who use the Internet to access the products offered by banks or fintech companies.

According to Molhova - Vladova, digitization is basically associated with creating, improving or transforming business processes through the use of digital technologies and digitized

data. (Molhova - Vladova, 2019) In this context, bank payment operations can be considered as a new way of implementing standard payment operations through the use of digital platforms and a set of tools for their implementation. The ultimate goal of all this is to achieve higher customer satisfaction and optimize the effectiveness of the products offered. Regarding the main objectives that can be achieved as a result of digitization in the banking sector Neikova states that they can be aimed at attracting new customers; the optimization of the prices of banking products and services; reducing customer service costs; better understanding of customer needs; the expansion of cross-selling. (Neikova, 2019)

These goals are also decisive in relation to the banks' responsibility, which in the changed business environment is even higher. Banks are on the front line supporting their customers during the crisis, both in their role as mediators of government stimulus actions and by making efforts to help customers with various solutions that optimize their work. Banks need to be aware of the reputational risk they face when customers feel they are not getting the support they need.

We believe that banks' behavior and maintaining good ethical standards will continue to be important to consumers' purchasing decisions. In support of this, Bellens cites the results of a study by Earnst&Yang, according to which more than half of respondents indicated that their future purchase decisions will be influenced by active support from banks, transparency in everything they do and ensuring that they do good for society. Conversely, 44% say purchasing decisions will be negatively impacted when they see banks focus on maximizing profits during this time. (Bellens, 2020)

An important aspect of the change in banking business models and the increasingly serious penetration of digitalization in relation to otherwise traditional banking services are the different types of risk that 'new' banking products/services carry. According to Gimblett, the use of digital channels leads to the development of existing risks and the emergence of new risks. That's why he believes risk managers will now spend more time identifying, assessing and mitigating them. We share the view that many of these risks are not really "new risks", they are evolving and increasing as a result of structural changes due to the digitization of business models and processes, as Gimblett points out. (Gimblett, 2018)

The change of banking business models in the way of introducing digital innovations, new ways of providing classic banking services and the entry into new territories, not inherent to traditional banking, is of key importance for the future development of the banking system. Similar conclusions are drawn by Lazarov, who makes the conclusion that "innovations in banking and new technological solutions have the potential to significantly change the business model in traditional retail banking (my italics R.M.) and that technological innovations have a significant impact on the profitability and efficiency of banks (Lazarov, 2022, p. 38). According to the author, the implementation of these innovations is related to the need for significant investments to implement the digital transformation of banks, which in turn leads to a change in the banks' strategies. An important point in this research is the conclusions regarding retail banking, which is developing at a very fast pace.

In this aspect, it should be noted that the regulatory environment in which banks operate has also changed in response to the ever-increasing processes of digitalization and the change in the intensity and significance of the risks associated with these processes. A kind of catalyst for the processes in this regard are the new European regulations, namely the Second Payment Services Directive (PSD2) and the accompanying extensive secondary legislation, which is mostly of a technical nature. Two aspects can be singled out as the main innovations in the Directive: opening access to payment accounts and increasing the requirements for the security of electronic payments. In relation to the implementation of the second aspect, the European Banking Authority (EBA) was authorized under Article 98(1) of Directive (EU) 2015/2366 (the Payment Services Directive or PSD2) to develop draft Regulatory Technical Standards (RTS) for highly client authentication and common and secure open communication standards (SCA&CSC). (European Commission, 2022)

The existence of a number of questions that were waiting for answers is often the basis of the designation of the directive as "one of the most significant developments" in the world of payment operations. As we have already indicated, the Directive introduces a new regulatory framework in the payment services segment, which is mainly aimed at their digitalization. This includes three main directions of regulation – liberalizing the market of payment services and facilitating the access of new players in it, ensuring security and reliability, as well as compliance with Community standards for the protection of personal data. The goal is to make the European market more competitive, to introduce more innovations, but at the same time to protect the interests of consumers as much as possible.

According to the texts of the Payment Services Directive, the changes in a purely technical aspect for banks come down to:

• Banks are obliged to provide third parties (primarily technology companies) with access to their customers' accounts, of course - with the consent of the customers themselves. This gives fintech companies the ability to transact from customer accounts as well as access vast data sets.

• The introduced requirement for Strong Customer Authentication, which aims to better protect users of payment services.

As a result of the introduced requirements, in practice, the new European directive is expected to contribute to the transformation of banks into technology companies, creating many new opportunities for them. According to Ismailov, banks should realize that they can partner with third party providers (TPP) and consider the transactions generated through them as a new channel, alternative and equal to mobile and internet banking. (Profit.bg, 2020) This, in turn, means not to put obstacles in front of the users of services through TRR, but to achieve at least the same level of customer experience as there is in the digital channels approved by the banks. At the same time, the discovery of new opportunities for banks is linked to the generation of new risks related to the implementation of this opportunities, to which bank managers should pay special attention.

Although financial risk management has improved significantly over the past 20 years, this has not been the case for other types of risk, such as operational risk and compliance risk, as they have not been among the most expensive (with large amounts of costs for banks). The large increase in fines, damages and legal costs over the past 5 years has forced banks to give them more importance. However, key risks such as cyber risk, model risk and contagion risk have emerged, which can be considered the three main types of risk associated with the digitization of business today.

In their June 2022 report, Mikkelsen et al. point out the increased risk of financial crime as an inevitable part of the burgeoning success of Payment Service Providers (PSPs). They believe that, unmanaged, this risk could pose an existential threat to PSPs, which in turn leads them to believe that weaknesses in the controls applied by electronic payment platforms will attract the attention of regulators. (Mikkelsen, et al., 2022) These conclusions, in our opinion, are very important in the context of PSD2, since in practice they give grounds to talk about the so-called "risk-forwarding" as a result of the interaction between banks and other service providers such as fintech companies for example. The question is how banks will be able to guarantee the security of their customers as a result of this transfer of risk, i.e. to manage the risk of the banking operations carried out, as PSPs are effectively already part of the payments value chain? That is why Mikkelsen et al. point out that regulators caution banks that facilitate payments on behalf of PSPs to validate the adequacy of PSPs' controls against financial crimes in their network of customers and partners (Mikkelsen, et al., 2022), which supports our “risk-forwarding” thesis.

The complex and changing business environment in which banks operate requires the bank managers to be extremely prescient about the future risks they may face. In support of this thesis, it was indicated in a Deloitte study that banks should develop more models to comply with parallel regulations, such as: implementation of the IFRS 9 framework and the applied perspective approach of expected credit losses; FRTB, IRB models and TRIM; Regular stress tests by the ECB (Deloitte,

2017), which shows that the environment and type of banking products/services offered predetermines the type and levels of risk they carry. The operational risk models described by Deloitte as the "loss allocation model" or the "integration model" can be used for regulatory, management and accounting purposes. (Deloitte, 2017, p. 15)

In fact, the risks posed by the digitization of banking processes and operations are of a different nature. Regardless of the fact that all these risks are actually arising from digitalization, we believe that their correct and timely recognition is of key importance for their management. Deloitte lists ten types of digital risks:(Deloitte, 2020)

- Cybersecurity risk
- Ecosystem risk
- Emerging technology risk
- Execution risk
- Fraud risk
- Privacy risk
- Legal and regulatory risk
- Brand and reputational risk
- Strategic risk
- People and culture risk

From the Toppr.com platform, they indicate another systematization of risks related to electronic banking: operational risk, security risk, reputational risk, legal risk, money laundering risk, cross-border risk and even strategic risk. (Toppr, 2022) According to the authors, operational risk or transaction risk is the most common type of risk in electronic banking. It may include incorrect processing of a transaction, compromises in data integrity, data confidentiality, unauthorized access to the bank's systems, non-fulfillment of contracts, etc. Here, we believe that the classification can be refined and some of the stated risks (e.g. reputational risk) can be included as part of the operational risk, but this does not fundamentally change our thesis.

All these types of risk and the specified aspects of risk may have their accounting projections, which are largely related to the recognition of losses in relation to certain items in the banks' financial statements. Carrivick and Cope acknowledge that some of the losses are not detected or reported until after the event has occurred due to fraudulent activities that were well hidden by the perpetrator.(Carrivick & Cope, 2013) Kopp et al. point out that IT - related and in particular cyber risks can be considered as a subset of operational risks as they are often cited as a significant threat to the financial system. According to the authors, the threat of this type of risk extends far beyond finance, as interest in cyberspace has gradually increased over time.(Kopp, et al., 2017)

All the risks mentioned above can occur due to some design flaws, insufficient technology, careless employees and unauthorized access to the system (intentional or not). It is therefore important that banks adopt the right technology and systems and have appropriate access controls for a secure transaction environment.

**2. Practice in disclosing the risk of digital payment services by some Bulgarian banks.**

It can be concluded that the risks associated with the digitalization of bank payment operations are an element of the bank's operational risk. As such, they can be expected to have an impact on the recognition of losses for the bank, but such losses that do not result from the application of the expected credit loss (ECL) model provided by IFRS 9, given the fact that there is effectively no balance sheet position to which this model to be applied, i.e. this is not credit risk. Rather, it is a risk of losses that are the result of some flaws in the design of the offered products/services, insufficiently reliable technologies, violation or neglect of internal control procedures by bank employees, unauthorized access to the system (intentional or not) etc. It is

therefore important that banks build and manage an adequate internal control system, as well as to ensure appropriate access control and a secure environment for carrying out transactions, both by the bank and by third party service providers within the meaning of PSD2.

Similar conclusions were drawn in the working paper of the Bank for International Settlements, according to which cyber losses represent a small fraction of total losses in terms of both gross amount and frequency. (Aldasoro, et al., 2020) Support for the shared thesis is also found in Kopp et al., whose research indicates that more than 90 percent of total cyber risk costs are attributable to indirect factors, with these costs occurring over time in all four phases of cyber risk management: Prevention, Reaction, Impact management and Business recovery and remediation. (Kopp, et al., 2017).

The accounting interpretation of risk in financial statements is regulated in IFRS 7. The standard requires companies to report in their financial statements the indicators they use internally to manage and measure financial risks. The standard defines three main risks: credit, market and liquidity risk. (IFRS 7) We believe that an important aspect of digital risk analysis is understanding the wider category of "financial risk". Although it is not a question of any of the three mentioned types of risk, the existence of the possibility that the bank may suffer direct losses or be forced to carry out significant unplanned expenses is a kind of manifestation of financial risk for the bank. In the context of financial statement disclosures, best practice banks are expected to provide stakeholders with a complete picture and clear understanding of the financial position, which includes not only information related to quantitative measures of potential impact on the financial statement, but also and the rationale for holding digital financial instruments and conducting banking operations in a digital environment in the context of the overall business and financial risk management strategy, of which the operational risk to which the bank is exposed is a part.

The scope of the study includes the five largest banks based on their total assets, grouped by the "Banking Supervision" department in the first group[1]: "UniCredit Bulbank" AD, "DSK Bank" AD, "United Bulgarian Bank" AD, "Eurobank Bulgaria" AD and "First Investment Bank" AD. For the purposes of the research, publicly available information from the banks' financial statements, the official websites of the banks under consideration, which includes offered banking products and services, the Tariff for the fees and commissions of the individual banks, specialized brochures, etc., was studied. The research methodology includes: a comparative analysis of the electronic payment services offered by the studied banks and an analysis of the disclosures in the financial statements related to the reporting of specific information about the risks associated with the digitalization of payment operations.

Table 1. Comparative analysis of bank payment services offered through electronic banking to individual customers

| **Bank** | | | **UniCredit Bulbank** | **DSK Bank** | **UBB** | **Eurobank Bulgaria** | **FiBank** |
|---|---|---|---|---|---|---|---|
| | **Electronic banking platform used** | | Bulbank Online | DSK Direct | UBB Online | Well - Postbank | My Fibank |
| | | *Performing a credit transfer in national or | Yes | Yes | Yes | Yes | Yes |

[1] The grouping does not contain elements of a rating and should not be interpreted as an assessment of their financial condition. The place of the banks in the individual groups depends on the size of their assets at the end of each reporting period. Banks in Bulgaria (January-March 2022). Bulletin of the BNB. https://bnb.bg/bnbweb/groups/public/documents/bnb_publication/pub_b_in_b_2022_03_bg.pdf , seen on 10/22/2022

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | | foreign currency | | | | | |
| | | *Payment of obligations for household (utility) services | Yes | Yes | Yes | Yes | Yes |
| | | * Creation (performing) periodic payments; | Yes | Yes | Yes | Yes | Yes |
| | **PAYMENT SERVICES** | *Currency exchange | Yes | Yes | Yes | Yes | Yes |
| | | *Payment of fees, receipts, taxes, etc. | Yes | Yes | Yes | Yes | Yes |
| | | *Bank card operations - application for issuance, repayment of credit card obligations, etc. | Yes | Yes | Yes | Yes | Yes |

Source: Official websites of the surveyed banks

The analysis of the information in the table1 shows that:

- Bulgarian banks have developed and maintain a wide range of electronic payment operations that customers can perform through the electronic banking platforms of the respective banks.
- There are six main types of payment operations that individual customers can carry out and which are practically offered by all banks, differing only in the design of the offered services and the individual fees that banks collect for their execution according to the established tariff of each bank.
- There are no specific requirements regarding the access of third parties (service providers) to bank customer accounts within the meaning of PSD2 that are relevant to the risk assessment in this aspect.

The development of the product portfolio and its constant addition, as well as the introduction of new payment systems, provoked by the development of the fintech industry, is also related to the development of the risks faced by banks. The accounting interpretation of risk is mainly associated with the recognition of specific losses related to the manifestation of a certain risk in the banks' activities, which leads to incurring additional costs and/or incurring direct default losses for the bank. Therefore, we believe that the disclosure of sufficiently complete and up-to-date information regarding these risks is of key importance for their understanding, assessment and management.

Table 2 provides a summary of specific disclosures in banks' financial statements:

Table 2. Disclosures related to the risk of digital payment operations in banks

| **Banks** | **Disclosures related to the risk of digital payment operations (cyber risk)** | |
|---|---|---|
| | **2020** | **2021** |
| UniCredit Bulbank | Yes, as part of operational risk<br>No financial effects | Yes, as part of operational risk<br>No financial effects |
| DSK Bank | Yes, as part of operational risk<br>No financial effects | It is not assigned to a specific type of risk<br>No financial effects |
| United Bulgarian Bank | Cyber risk / information security, which is part of operational risk<br>No financial effects | Cyber risk / information security, which is part of operational risk<br>No financial effects |
| Eurobank Bulgaria | 4 types of risk are defined, including operational risk without detailed disclosure of cyber risks<br>No financial effects | 4 types of risk are defined, including operational risk without detailed disclosure of cyber risks<br>No financial effects |
| First Investment Bank | Yes, as an element of operational risk<br>No financial effects | Yes, as an element of operational risk<br>No financial effects |

Source: Financial statements of the surveyed banks for the period 2020-2021.

The analysis of the information in table 2 allows the following conclusions to be drawn:

- It is noteworthy that all banks directly or indirectly treat cyber risks as an element of operational risk.
- Almost all banks use the same definition of operational risk, considering operational risk to be the risk of loss arising from inappropriate or faulty processes, people or systems, or from external events.
- In order to reduce the risks arising from various adverse events (risks), banks apply written policies, have introduced rules and procedures that are based on requirements laid down in European and Bulgarian legislation, as well as good banking practices.

- Regarding the capital requirements for operational risk, the studied banks apply the standardized approach according to the requirements of Regulation (EU) No. 575/2013, as in this regard, for example, FiBank has also specified a methodology for distributing the indicators by groups of activities.[2]
- There is a lack of differentiated disclosures regarding incurred costs and/or reported losses from the occurrence of cyber risks related to digital products and services and, in particular, to digital payment operations. Such a lack can be explained either by the insignificant values of these costs/losses, or by the lack of practice for reporting the financial effects of the occurrence of the various types of risks (other than credit risk) in the banks' financial statements.

**Conclusion**

The development of banking business models as a result of the advent of digital technologies has significantly changed the way banks perform even traditional operations. At the same time, this change is associated with new risks that bank managers must know and manage. Very often, the cyber risks that are inherent in the digitalization of business processes are reduced only to malicious attacks against the bank and/or its customers, but in many cases these risks are related to reputational risk, which is of very high importance for banks in highly the competitive environment in which they operate. In cases where e-banking problems occur, where a bank fails to perform critical functions or does not perform as per the expectations of its customers, then it faces the risk of reputational loss, which ultimately leads to loss of customers and incurring financial losses. Even reasons for this risk are a system or product that does not function as expected, significant system flaws, security breaches (external or internal), improperly informing customers about the processes and policies of using e-banking, certain communication problems that prevent the customer from accessing his account, difficulties created in the access of third party providers to accounts of customers of the bank within the meaning of PSD2 etc., then this risk has its financial dimensions.

For this reason, we consider that the differentiated disclosure of the costs and/or reported losses from the occurrence of cyber risks in the financial statements of banks related to digital products and services and in particular to digital payment operations is necessary in order to properly defining, evaluating and analyzing these risks by all users of financial information.

**References**

1. Aldasoro, I., Gambacorta, L., Giudici, P. & Leach, T., 2020. BIS Working Papers No 840: Operational and cyber risks in the financial sector, Basel: BIS.
2. Bellens, J., 2020. Four ways COVID-19 is reshaping consumer banking behavior. [Online] Available at: https://www.ey.com/en_us/banking-capital-markets/four-ways-covid-19-is-reshaping-consumer-banking-behavior [Accessed 10 11 2022].
3. Carrivick, L. & Cope, E., 2013. Effects of the financial crisis on banking operational losses. Journal of Operational Risk, 8(3), pp. 3-29.
4. Deloitte, 2017. Model Risk Management. [Online] Available at: https://www2.deloitte.com/content/dam/Deloitte/fr/Documents/risk/deloitte_model-risk-management_plaquette.pdf [Accessed 28 10 2022].

[2] Methodology for distributing the indicators by activity groups https://www.fibank.bg/web/files/documents/469/files/549300UY81ESCZJ0GR95-20211231-BG-SEP.xhtml , viewed on 20.11.2022.

5. Deloitte, 2020. Financial services: Managing risk to get fit for a digital future, sl: Deloitte Touche Tohmatsu Limited.
6. European Commission, 2022. COMMISSION DELEGATED REGULATION (EU) of 3.8.2022 amending the regulatory technical standards laid down in Delegated Regulation (EU) 2018/389 as regards the 90-day exemption for account access. [Online] Available at: https://ec.europa.eu/finance/docs/level-2-measures/psd2-rts-2022-5517_en.pdf
7. Gimblett, R., 2018. Operational risk management in the digital era in the Swiss banking industry, Geneva: Haute ecole de gestion - Geneve.
8. IFRS 7 — Financial Instruments: Disclosures: IASB.
9. Kopp, E., Kaffenberger, L. & Wilson, C., 2017. WP/17/185: Cyber Risk, Market Failures, and Financial Stability, sl: International Monetary Fund.
10. Mikkelsen, D., Rajdev, S. & Stergiou, V., 2022. Managing financial-crime risks in digital payments. [Online] Available at: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/managing-financial-crime-risk-in-digital-payments
11. Profit.bg, 2020. What should we know about the European payment directive PSD2?. [Online] Available at: https://profit.bg/kompanii/kakvo-tryabva-da-znaem-za-evropeyskata-platezhna-direktiva-psd2/ [Accessed 3 11 2022].
12. Toppr, 2022. Risks_of_E-Banking. [Online] Available at: https://www.toppr.com/guides/business-economics-cs/money-and-banking/risks-of-e-banking/#Risks_of_E-Banking
13. BNB, 2022. Banks in Bulgaria April - June 2022, Sofia: Bulgarian National Bank.
14. Lazarov, N., 2022. Inovatsii v bankiraneto na drebno i priloyenieto im v Balgariya - perspektivi i tendentsii (Avtoreferat na disertatsionen trud), Sofiya: VUZF.
15. Molhova - Vladova, M., 2019. Internatsionalizatsiya na predpriyatiyata v usloviyata na digitalna transformatsiya na biznesa. Industrialni otnosheniya i obshtestveno razvitie, Br. 2.
16. Neykova, M., 2019. Razvitie na inovatsiite i tehnologiite v bankoviya sektor. Proceedings of the International scientific and practical conference “Bulgaria of regions’2019” Plovdiv ss. 401-406
17. NSI, 2021. Litsa, izpolzvashti internet za lichni tseli. [Online] Available at: Лица, използващи интернет за лични цели | Национален статистически институт (nsi.bg)