MITIGATING RISKS IN OPEN BANKING

Ela Mădălina SCARLAT[40]

Abstract: *The implementation of open banking has revolutionized the financial services landscape, enabling data sharing and collaboration among financial institutions, fintechs, and third-party providers. While promoting financial inclusion and fostering innovation and competition, open banking presents inherent risks that necessitate identification and mitigation for sustainable growth.*

To promote financial inclusion and prevent fraud, establishing digital identities and proper customer identification, including biometric measures, is crucial. However, the complexity of European legislation on authentication and transaction security necessitates unified global standards.

A comprehensive risk mitigation framework must encompass robust security measures, third-party due diligence, continuous monitoring, best practices, and effective incident response plans. Transparent customer consent and awareness are also vital for secure open banking implementations.

Collaborative efforts among stakeholders and strong regulatory oversight are necessary to navigate open banking's long-term implications, including cross-border collaboration and global data sharing through harmonized regulatory frameworks.

By adopting these measures and fostering collaborative efforts, financial institutions can effectively manage risks and ensure the sustainable development of open banking initiatives, advancing financial inclusion and bolstering the interconnected digital economy.

Keywords: *open banking, financial inclusion, risk assessment, cyber risk, financial institutions*

JEL Classification: *E4; E42; E5; E58.*

[40] Romanian Academy, "Costin C. Kiriţescu" National Institute of Economic Research, Bucharest, Romania, e-mail: ela.scarlat@bnro.ro

Introduction

Globalization has profoundly shaped the world's economies, resulting in increased interaction, interconnection, and interdependence between nations. The financial-banking sector, in particular, has evolved into a borderless realm, allowing consumers to access goods and services from anywhere globally. This transformation has been further accelerated by the advent of the internet and the growth of online commerce, leading to a significant expansion of the digital payment market.

In Romania, ensuring financial stability and sustainable development requires the creation of efficient, rapid, and secure channels for capital circulation. This entails maintaining the integrity, operability, and continuity of payment infrastructures and enforcing market discipline among participants. Embracing innovative payment services, instruments, and infrastructure becomes essential to building resilient systems, promoting sustainable industrialization, and encouraging innovation, all of which contribute to a well-functioning economy.

Digitization offers numerous advantages, including increased efficiency and productivity for financial institutions, reduced operational costs, a wider range of financial products and services for consumers, and enhanced market competitiveness. Moreover, digital payments can help combat the underground economy, fostering transparency and accountability.

Several trends are reshaping payment methods worldwide. These include the widespread acceptance of digital payments, the rise of instant payments as the new norm, and the emergence of internet-based payment infrastructures, which create opportunities for new business models and non-bank providers like FinTech and BigTech companies. Stablecoins and central bank digital currencies (CBDCs) have also garnered attention, revolutionizing payment systems and potentially leading to rapid global adoption.

To achieve efficient, secure, and accessible payment systems, technology plays a pivotal role. Utilizing artificial intelligence and digital identities

can address imperfections, reduce transaction costs, and improve trust-based services. Standardization and interoperability are crucial to ensuring seamless payment transactions and enhancing cybersecurity to safeguard against potential threats in an interconnected financial ecosystem.

The European Union (EU) has taken initiatives to strengthen retail payments, promoting the free movement of capital within its borders and beyond. The Single Euro Payments Area (SEPA) facilitates cross-border payments, benefiting countries like Romania, which depend on low-cost remittance transfers from abroad. However, various challenges, such as data standardization, compliance complexity, and outdated technology, hinder the seamless process of cross-border payments.

In this context, the EU's retail payments strategy aims to develop pan-European payment solutions and support instant payments, innovation, and ecological sustainability. As instant payments become the new standard, Romania must actively encourage all banks to participate in the instant payment system to benefit from its advantages fully.

Amidst these developments, open banking emerges as a progressive approach revolutionizing the financial services industry. By allowing secure data sharing through APIs (Application Programming Interfaces), open banking empowers consumers with greater control over their financial information and access to tailored and innovative financial products and services. However, the adoption of open banking also introduces new risks that demand careful consideration and proactive risk mitigation strategies.

The evolution of the financial-banking sector towards a borderless and digitized landscape, driven by open banking and other transformative technologies, offers immense opportunities for economic growth and financial inclusivity. Nevertheless, it is crucial for policymakers and stakeholders to strike a balance between leveraging the potential benefits and managing the associated risks to ensure a resilient and sustainable financial ecosystem for all.

Literature review

BIS (2019) defines Application Programming Interfaces (APIs) as a set of rules and specifications for software programs to communicate with each other, that forms an interface between different programs to facilitate their interaction.

Open API is an interface that provides a means of accessing data based on a public standard and it is also named as external or public API (BIS, 2019). Open Banking refers to a practice in the financial industry where banks permit regulated third-party providers (TPPs) to access bank customer data, subject to the customer's consent. This data sharing is made possible through Application Programming Interfaces (APIs), enabling TPPs to offer a wide array of innovative technologies, applications, and services. The shared financial data may encompass payment initiation, statements, and transaction records.

The existing definitions of open banking face three fundamental problems: perspective bias, discipline bias, and purpose bias. Perspective bias occurs when the tripartite scheme involving the data owner, custodian, and third party accessing it is not fully considered in general definitions, leading to partial analysis. Discipline bias arises from researchers confusing the context in which open banking is used in their field, leading to narrow definitions focusing only on specific aspects. Purpose bias occurs when open banking is given a specific purpose other than its intended goal of increasing competition in retail banking. These biases combined hinder the construction of solid and generalizable knowledge about open banking, which is a significant limitation for its development (Briones de Araluze, Cassinello Plaza, 2023).

Open banking offers numerous opportunities, including enhanced customer experiences, increased innovation, and financial inclusion. However, these advantages coexist with risks, such as data breaches, cyber-attacks, and the misuse of customer data, that need to be addressed. Data security and privacy remain paramount, requiring robust cybersecurity measures and compliance with stringent regulatory standards. Building customer trust is vital, and financial institutions must

ensure transparent and user-friendly consent processes. Additionally, interoperability between different APIs and systems must be established for a seamless open banking experience.

Open banking has the potential to boost financial inclusion by providing underserved populations with access to affordable and tailored financial solutions. The integration of open banking with emerging technologies like Artificial Intelligence and Machine Learning can lead to innovative financial products and services, catering to specific customer needs and preferences.

Countries worldwide have been embracing open banking to varying degrees, driven by different regulatory frameworks. In Europe, the Revised Payment Services Directive (PSD2) has been a pivotal driver for open banking adoption, mandating financial institutions to provide access to customer data through APIs. Other regions, such as Australia and Canada, have also introduced open banking initiatives to promote competition and innovation in the financial sector.

APIs play a central role in facilitating data sharing between financial institutions and third-party providers. They act as bridges that enable seamless communication between different systems, allowing for real-time access to customer data while maintaining data security and privacy.

The foundation of open banking is built on four key principles: customer consent, data privacy, security, and competition. These principles ensure that customers have full control over their data, with the ability to grant or revoke consent for data sharing, and that the highest standards of data security and privacy are maintained.

Open Banking in Europe is facilitated by the EU's regulation known as PSD2, which stands for Payment Services Directive 2. This directive, issued by the European Union, mandates that banks must grant TPPs access to their customer data and payment systems.

The primary objective of PSD2 is to enhance competition, foster innovation, and improve safety within the payment services industry. By complying with PSD2, customers can securely share their financial data

with TPPs. Consequently, customers gain the ability to compare various financial products and services available in the market, empowering them to make informed choices that best suit their individual needs. However, GDPR rules limit universal access and control over data by third parties.

Open Banking and PSD2 offer several key advantages that drive innovation and transformation in the financial services industry. The main benefits include:

- increased competition: open banking allows new players to enter the market and offer innovative financial products and services to consumers, challenging traditional banks and fostering healthy competition.
- enhanced financial services: PSD2 mandates banks to provide third-party providers (TPPs) with access to customer data, enabling the creation of more convenient and user-friendly financial services.
- improved financial inclusion: Open Banking can promote financial inclusion by making it easier for underserved communities to access financial services.
- heightened security: PSD2 incorporates strong security requirements to safeguard customer data. Banks must use secure communication and robust customer authentication methods to grant access to financial information.
- transparent and efficient payments: open banking and PSD2 promote faster, more secure, and transparent payment services, reducing the time and costs associated with traditional banking services.

The process of open banking involves the implementation of APIs, allowing secure access to a customer's financial information for authorized TPPs. Customers must give consent for TPPs to access their data and initiate payments on their behalf. The bank authenticates the TPP and ensures secure data transmission. Strong customer authentication (SCA) is employed to protect against fraud.

While open banking and PSD2 have been designed with security in mind, there are still potential risks, and customers should take

precautions to protect their financial information. SCA, required by PSD2, involves two-factor authentication to enhance security during electronic transactions.

The future of open banking is expected to witness continued growth, adoption, and increased regulatory scrutiny. API standardization, improved security measures, and heightened competition between banks and fintech companies will likely be key trends. A revision of PSD2, known as PSD3, is in progress and may extend the validity of consents and provide access to other types of accounts, further advancing the evolution of open banking and the accessibility in the financial system.

This paradigm shift in the financial services industry brought about by open banking has redefined the entire financial landscape. By fostering greater financial transparency and facilitating personalized services, open banking holds the potential to revolutionize how customers interact with financial institutions.

However, alongside its numerous benefits, open banking also introduces new risks that require careful consideration and proactive risk mitigation strategies. Data sharing and API-enabled access raise concerns about data privacy, security, and the potential misuse of sensitive financial information. As such, ensuring robust cybersecurity measures and strict adherence to data protection regulations becomes imperative.

Despite these challenges, the advantages of open banking are significant. It can enhance competition, drive innovation, and promote the development of customer-centric financial products and services. By allowing non-traditional players like FinTech and BigTech companies to participate in the financial ecosystem, open banking paves the way for greater inclusivity and accessibility to financial services.

Romania's digital economic development, measured by DESI, shows strengths in the private sector but weaknesses in digital skills. Measures to bridge gaps, increase digital literacy, and promote financial education can improve financial inclusion. Promoting technological neutrality, open banking, and secure digital identification is crucial for advancing

digital payments and financial inclusion while addressing cybersecurity challenges.

In order to harness the full potential of open banking while effectively managing associated risks, collaboration between financial institutions, regulators, and third-party service providers is essential. Establishing clear guidelines, standards, and protocols for data sharing and customer consent can ensure that open banking operates in a secure and responsible manner.

Moreover, promoting financial literacy and educating consumers about the benefits and risks of open banking is vital to building trust in this new financial landscape. Encouraging consumers to make informed decisions and exercise their control over data sharing can lead to a more empowered and financially resilient society.

Therefore, open banking represents a significant step towards a more consumer-centric and innovative financial ecosystem. By embracing this collaborative approach, the financial services industry can unlock new opportunities for growth and drive greater financial inclusion. Nevertheless, it is crucial for all stakeholders to work together to address the challenges and risks associated with open banking, safeguarding the interests and data privacy of consumers while fostering a thriving and secure financial environment.

Innovation can be fostered through technological neutrality, ensuring equal opportunities for consumer access to the internet, smartphones, and other technologies without discrimination based on the technology used.

The EU introduced DORA to support innovation and protect consumers and to establish a regulatory framework for digital operational resilience.

National supervisory authorities vary in their approach to authorizing FinTech business models, with some countries offering dedicated programs like sandboxes, while others take a more conservative approach.

Technologies like AI (artificial intelligence)/ML (machine learning), DLT and CBDCs present opportunities to improve cross-border payments, combat money laundering, and enhance back-end processes. However, challenges such as fragmented data and existing constraints need to be addressed.

Unique digital identification is crucial for fraud prevention in digital payments, and digital identity systems must adhere to technical and legal standards while protecting individual privacy and avoiding discrimination.

Ensuring data and cyber security in open banking is challenging due to the increased surface area for cyber attacks caused by data sharing with third parties, leading to the need for effective data management. The development of APIs to share customer-permissioned data faces challenges, including the time, cost, and lack of commonly accepted standards, impacting universal adoption (BIS, 2019).

To succeed in adopting new payment technologies, financial authorities need to strike a balance between fostering innovation and ensuring consumer protection and financial stability.

Information Sharing and Analysis Centers (ISACs) play a vital role in exchanging information on cyber threats.

A comprehensive cybersecurity strategy is essential for institutions, involving risk assessment and cost-benefit analysis.

Oversight of third parties in open banking can be limited, especially when there are no contractual relationships with banks, raising concerns about data sharing and potential unauthorized data sharing by third parties. Assigning liability in case of financial loss or erroneous sharing of sensitive data is complex in open banking due to multiple parties and intermediaries involved in providing financial services. Banks may face reputational risk, even in jurisdictions with established liability rules, as customers rely on banks to safeguard their data, and any breaches can impact customer trust and confidence (BIS, 2019).

Methodology

The qualitative research methodology employed in this study involves a comprehensive review and analysis of relevant specialized literature and legislaiton pertaining to financial inclusion, cyber resilience, and risk management in the context of the digital economy, specifically focusing on open banking and payment systems. The research methodology integrates practical studies, theoretical analysis, and logical discourse to establish an understanding of the challenges and best practices associated with cyber-risk assessment and mitigation, aiming to enhance financial inclusion while safeguarding payment systems against evolving cyber threats.

The data for this research was collected through a systematic search of scholarly articles, research papers, industry reports, regulatory documents, and relevant legislative frameworks related to financial inclusion, open banking, cybersecurity, and risk management. Online databases, academic journals, and authoritative sources in the fields of finance, cybersecurity, and digital payments were consulted to ensure the inclusion of the most recent and reliable information. The collected data was subjected to rigorous qualitative analysis techniques, including thematic analysis and content analysis, to identify recurring themes, patterns, and insights related to cyber risk assessment, vulnerability identification, risk mitigation, operational resilience, interdependency risks, and the integration of security and recovery measures in payment systems.

Based on the analysis of the literature and legislation, a general and structured framework that addresses the challenges faced by financial institutions and payment service providers in ensuring cyber resilience and financial inclusion was developed. This framework advocates a risk-based approach, taking into account the identified vulnerabilities, threats, and potential impacts on payment systems, thereby allowing for the optimal allocation of resources for security measures and recovery capabilities.

The qualitative approach was chosen for this research due to its ability to provide a deep understanding of complex phenomena, such as financial inclusion and open banking, and to explore and gain insights into the challenges and best practices associated with cyber-risk management and payment system security. Qualitative research allows for a nuanced examination of various risk factors, vulnerabilities, and potential impacts on payment systems, enabling a more holistic perspective on cyber resilience in the digital economy.

By employing qualitative research methodologies and conducting a comprehensive review of relevant literature and legislation, this study aims to contribute valuable insights to the field of cyber resilience, financial inclusion, and risk management in the context of open banking and digital payments. The findings of this research will be instrumental in guiding financial institutions, policymakers, and regulators in developing effective strategies and measures to address cyber threats, enhance financial inclusion, and ensure the secure and sustainable development of open banking initiatives in Romania and beyond.

Results and discussions

Digital economy cannot be fully implemented until the issue of financial exclusion is addressed, especially in rural areas. A significant portion of the population in Romania is not ready for safe digital payments, lacking the necessary knowledge for basic "cyber hygiene." Overcoming barriers to financial inclusion can be achieved through specific programs targeting certain population groups and specific areas that require support and intervention to bridge the gaps, enhance digital literacy, and improve financial education.

The major challenges for the national economy resulting from the digitization of payments are as follows:

– cybersecurity risks: Both payment systems and participants within the financial ecosystem, critical or non-critical, are exposed to cyber threats. To mitigate these risks, common cybersecurity standards are

necessary for all participants, and their consistent application, respecting the principle of proportionality, is crucial.

- prioritizing financial education: Providing financial literacy (and digital literacy to all users) is essential. This can be achieved through various programs, possibly funded by the government, and by using digital solutions (applications) to inform users about new products and services, benefits, risks, and risk mitigation practices.
- strong preference for cash: Romanians have a clear preference for cash, much more pronounced than in other European countries. Eliminating cash is not recommended as it would disproportionately affect the poor and elderly who rely on it. There is also a social value to cash for those who lack smart devices to use payment applications.

Digital identity creation and proper customer identification, such as biometric identification, are the first steps toward increasing financial inclusion through digitization and preventing fraud. However, the complexity of European legislation on authentication and transaction security requires careful consideration, as unified global standards are lacking.

The effects of implementing open banking are synthetized below:

- open banking has revolutionized the financial services landscape by promoting data sharing and collaboration among financial institutions, fintechs, and other third-party providers. However, this open and interconnected environment also presents inherent risks that must be identified and addressed to ensure the sustainable growth of open banking;
- promoting financial inclusion: open banking has the potential to bridge the financial inclusion gap by expanding access to financial services for underserved populations. Increased data availability allows financial institutions and fintechs to assess the creditworthiness of individuals who were previously excluded from traditional banking systems;
- fostering innovation and competition: the adoption of open banking has paved the way for innovative collaborations between traditional financial institutions and fintech startups. Increased competition

within the financial sector has incentivized institutions to enhance their product offerings and customer experiences, driving overall industry innovation;

- customer-centric services: open banking encourages financial institutions to focus on customer needs, leading to the development of personalized and customer-centric services. Tailored financial products and services can be designed based on customer data, improving customer satisfaction and loyalty;
- challenges and risks: while open banking offers numerous advantages, it also presents challenges and potential risks. Cybersecurity threats, data breaches, and unauthorized access to sensitive information are primary concerns that demand robust security measures. Customers' data privacy and the need for transparent consent processes require stringent regulatory oversight.
- regulatory frameworks: strong regulatory frameworks play a pivotal role in governing open banking initiatives. Regulators must strike a balance between promoting innovation and protecting customer interests. Standardized guidelines and compliance measures are essential to ensure data security and consumer trust;
- collaborative efforts: Open banking requires collaboration among financial institutions, fintechs, regulators, and other stakeholders. Information sharing and open dialogue can help identify emerging risks and devise effective risk mitigation strategies;
- business model transformation: the implementation of open banking necessitates a transformation in traditional business models. Financial institutions must adapt to the changing landscape by adopting API-driven technologies, embracing collaboration, and prioritizing customer-centricity;
- long-term implications: the long-term implications of open banking are multi-faceted. Continued innovation and competition could lead to increased financial accessibility, efficiency, and customer satisfaction. However, monitoring and addressing potential negative

impacts are crucial to maintain a stable and sustainable financial ecosystem.

As open banking continues to evolve, the potential for cross-border collaboration and global data sharing becomes more apparent. Standardization and harmonization of regulatory frameworks across regions can unlock new opportunities for international expansion and promote a more interconnected financial ecosystem.

Risks of open banking:

- data breaches: the interconnected nature of open banking creates an expanded attack surface, increasing the risk of data breaches and unauthorized access to sensitive customer information. One of the primary risks associated with open banking is the potential exposure of sensitive customer data to cyber threats;
- fraud: open banking ecosystems can become susceptible to fraudulent activities, including account takeovers and identity theft, potentially causing financial losses to customers and financial institutions. Open banking introduces new opportunities for fraudsters to exploit vulnerabilities in the system. The use of strong customer authentication mechanisms, transaction monitoring, and fraud detection algorithms can help mitigate the risk of fraudulent activities. Financial institutions should collaborate with third-party providers to establish standardized security protocols and conduct regular audits to identify potential security gaps;
- privacy concerns: the vast amount of shared customer data raises privacy concerns, necessitating strict adherence to data protection regulations and customer consent requirements;
- third-party risks: collaboration with third-party providers introduces new risks, as their security measures and practices may not align with industry standards, leading to potential vulnerabilities.

Robust data security measures, including encryption, multi-factor authentication, and regular vulnerability assessments, are critical to safeguard customer information. Compliance with data protection

regulations, such as GDPR and CCPA, is equally essential in maintaining data privacy.
A comprehensive risk mitigation framework should be based on:

- Robust Security Measures:

– Implement stringent cybersecurity protocols, including encryption and multi-factor authentication. Financial institutions must implement robust security protocols, such as multi-factor authentication, encryption, and tokenization, to safeguard customer data and prevent unauthorized access;
– Continuous monitoring and threat intelligence sharing are essential to identify and respond promptly to emerging cybersecurity threats;
– Conduct regular risk assessments to identify vulnerabilities and address them promptly;
– Utilize big data analytics to detect potential fraudulent activities and monitor transactions effectively;
– Maintain a robust API governance framework with strict access controls and audit trails;

- Third-Party Due Diligence:

– Financial institutions must conduct thorough due diligence when selecting third-party providers for collaboration. Assessing their security protocols, compliance with regulations, and financial stability helps minimize risks associated with partnering with third parties;

- Continuous Monitoring, Assessment and Compliance:

– Continuously monitor and update cybersecurity protocols and regulatory compliance measures;
– Stay informed about emerging threats, regulatory changes, and industry best practices;
– Build scalable and agile systems to accommodate future advancements and customer needs;

- Evolving risk management strategies to adapt to changing threats and requirements;

- Best Practices and Incident Response:

- Developing a robust incident response plan allows financial institutions to act swiftly in the event of a security breach or data incident, minimizing the impact on customers and operations. Relevant drills to test effectiveness are also needed;

- Regular training and simulations enable employees to be prepared for potential threats and respond effectively;

- Transparent Customer Consent:

- Ensuring clear and explicit customer consent for data sharing is crucial in building trust. Institutions should provide easy-to-understand consent mechanisms and allow customers to revoke consent at any time;

- Ensure transparent and user-friendly consent mechanisms to empower customers;

- Educating customers about the benefits and risks of open banking fosters informed decision-making;

- Customer Awareness and Education:

- Providing customers with tools and resources to monitor and manage their data sharing preferences enhances their control over their financial information;

- Providing accessible and comprehensive educational materials, including FAQs and interactive platforms, enables customers to make informed decisions about data sharing and consent;

- Collaborative Efforts Among Stakeholders:

- Open banking requires a collaborative effort among financial institutions, fintechs, regulators, and customer advocacy groups. Information sharing, best practice sharing, and open dialogue can

help identify emerging risks and devise effective risk mitigation strategies;

- Collaboration between financial institutions, third-party providers and regulators promotes the exchange of best practices and insights on risk management;
- Establishing industry-wide cybersecurity standards and guidelines ensures a cohesive approach to addressing common risks;
- Establishing clear and comprehensive regulatory frameworks governing data sharing and customer protection;
- Collaborating with fintech innovators and academia to drive responsible innovation;

• Incident Response and Contingency Planning:

- Having a well-defined incident response plan is crucial to minimize the impact of potential data breaches or security incidents. Regular drills and simulations of various scenarios enable financial institutions to respond promptly and effectively to mitigate damages;

• Regulatory Compliance:

- A robust regulatory framework is fundamental to the successful implementation of open banking. Regulators must set clear guidelines and standards for data sharing, security, and customer protection. Financial institutions and third-party providers must adhere to these regulations to ensure a level playing field and to enhance overall industry stability;

• Strong Regulatory Oversight:

- Regulatory bodies play a pivotal role in ensuring compliance with data protection and privacy regulations. Institutions must adhere to industry-specific standards and frameworks such as PSD2 (in Europe) to enhance data security and customer protection.
- Regular audits and assessments by regulatory authorities help identify and rectify any lapses in security and compliance.

By implementing these measures and fostering collaborative efforts, financial institutions can effectively manage risks and ensure the sustainable development of open banking initiatives.

Conclusion

Open banking represents a paradigm shift in the financial services industry, reshaping the way financial institutions operate and interact with customers and third-party providers. The core principle of open banking revolves around data sharing and collaboration, enabling customers to grant explicit consent for their financial data to be accessed by authorized third parties. This new model promises a host of benefits, including enhanced customer experiences, increased innovation, and improved financial inclusion.

Gaining and maintaining customer trust is paramount in open banking. Transparent and user-friendly consent mechanisms are crucial to ensuring customers understand the data-sharing processes and retain control over their data. Clear communication regarding the benefits and risks of open banking fosters customer confidence in the system.

Given the critical nature of payment systems for national economies and the efforts to interconnect national payment ecosystems for improved cross-border payments, cybersecurity risk becomes increasingly important. Cybersecurity must be integrated into all digital investments, particularly essential technologies such as Artificial Intelligence (AI), encryption, quantum computing, and distributed ledger technology.

While open banking offers transformative potential, it also introduces inherent risks that must be effectively managed to ensure its sustainable growth in the digital age. One of the primary concerns is data security and privacy. With increased data sharing and connectivity between banks and various parties, the risk of cyber threats and data breaches escalates. Robust data security measures, such as encryption, multi-factor authentication, and regular vulnerability assessments, are critical to safeguard sensitive customer information. Moreover, compliance with

data protection regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), is equally essential to maintain data privacy and customer trust.

Another challenge lies in fraud and unauthorized access. The open and interconnected environment of open banking provides new opportunities for fraudsters to exploit vulnerabilities in the system. To counter this risk, financial institutions must implement strong customer authentication mechanisms, transaction monitoring, and fraud detection algorithms. Collaborating with third-party providers to establish standardized security protocols and conducting regular audits can help identify potential security gaps and mitigate fraudulent activities.

Customer trust and consent management are paramount in open banking. Gaining and maintaining customer trust is fundamental to the success of this model. Transparent and user-friendly consent mechanisms are crucial to ensure that customers fully understand the data-sharing processes and retain control over their data. Clear communication regarding the benefits and risks of open banking fosters customer confidence in the system.

In the digital era, cybersecurity is the cornerstone of risk mitigation. Financial institutions and third-party providers must invest in state-of-the-art cybersecurity technologies and expertise to protect their systems from cyber threats. Continuous monitoring, threat intelligence sharing, and incident response plans are vital components of a strong cybersecurity posture.

A robust regulatory framework is fundamental to the successful implementation of open banking. Regulators play a crucial role in setting clear guidelines and standards for data sharing, security, and customer protection. Financial institutions and third-party providers must adhere to these regulations to ensure a level playing field and enhance overall industry stability.

Cybersecurity measures are the cornerstone of risk mitigation in the digital era. Financial institutions and third-party providers must invest in state-of-the-art cybersecurity technologies and expertise to protect their

systems from evolving cyber threats. Continuous monitoring, threat intelligence sharing, and well-defined incident response plans are vital components of a strong cybersecurity posture.

Educating customers about open banking, its benefits, and associated risks is crucial to promoting responsible use and fostering trust. Providing accessible and comprehensive educational materials, including FAQs and interactive platforms, enables customers to make informed decisions about data sharing and consent.

Collaboration among financial institutions, fintechs, regulators, and customer advocacy groups is vital in navigating the challenges of open banking. Information sharing, best practice sharing, and open dialogue can help identify emerging risks and devise effective risk mitigation strategies.

Financial institutions must conduct thorough due diligence when selecting third-party providers for collaboration. Assessing their security protocols, compliance with regulations, and financial stability helps minimize risks associated with partnering with third parties.

Having a well-defined incident response plan is crucial to minimize the impact of potential data breaches or security incidents. Regular drills and simulations of various scenarios enable financial institutions to respond promptly and effectively to mitigate damages.

In conclusion, open banking offers transformative potential in the financial services industry. However, to fully realize its benefits, addressing data security, privacy, and regulatory challenges is essential. By embracing collaborative efforts, ensuring strong regulatory oversight, and prioritizing risk management measures, financial institutions can harness the transformative potential of open banking while safeguarding the interests of customers and industry stability. A proactive and comprehensive risk management framework is fundamental to ensuring the sustainable success of open banking in the ever-evolving financial landscape.

Romania should prioritize the capacity to detect cyber threats to minimize the impact of potential cyberattacks. Partnerships between state authorities, the private sector, and civil society are essential in creating a secure cyberspace.

Every organization and individual using the internet plays a role in ensuring a secure cyber transformation.

References

Achord, S., Chan, J., Collier, I., Nardani, S., Rochemont, S., A Cashless Society. Benefits, Risks and Issues (Interim Paper), Institute and Faculty of Actuaries, November 2019, https://www.actuaries.org.uk/system/files/field/document/A%20Cashless%20Society-%20Benefits%2C%20Risks%20and%20Issues%20%28Interim%20Paper%29%20-%20disclaimer.pdf

Aldasoro, I.; Frost, J.; Gambacorta, L.; Whyte, D. (2021), Covid-19 and cyber risk in the financial sector, Bank for International Settlements, January, https://www.bis.org/publ/bisbull37.pdf

Amir, E.; Levi, S.; Livne, T., (2018), Do firms underreport information on cyberattacks? Evidence from capital markets, Review of Accounting Studies, Vol. 23, Issue 3, No 11, https://econpapers.repec.org/article/sprreaccs/v_3a23_3ay_3a2018_3ai_3a3_3ad_3a10.1007_5fs11142-018-9452-4.htm

Aramonte, S.; Huang, W.; Schrimpf, A., (2021), DeFi risks and the decentralisation illusion, Bank for International Settlements, December, https://www.bis.org/publ/ qtrpdf/r_qt2112b.pdf

Arslanian, H.; Fischer, F., The future of finance. The impact of Fintech, AI and crypto on financial services, Editura Palgrave Macmillan, 2019, ISBN 978-3-030-14532-3

Auer, R.; Banka, H.; Boakye-Adjei, N.Y.; Faragallah, A.; Frost, J.; Natarajan, H.; Prenio, J. (2022), Central bank digital currencies: a new tool in the financial inclusion toolkit?, Financial Stability

Institute Insights on policy implementation No 41, April, https://www.bis.org/fsi/publ/insights41.pdf

Aysan, A.; Nanaeva, Z.; Shirazi, N.S. (2019). Open Banking from EU's Payment Services Directive to Practice: The Cases of Solarisbank and Insha, November, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3967612

Banca Naţională a României, Regulament nr. 2/2020 privind măsurile de securitate referitoare la riscurile operaţionale şi de securitate şi cerinţele de raportare aferente serviciilor de plată

Banca Naţională a României, (2022), Regulamentul nr. 6 din 12 aprilie 2022 privind cadrul de desfăşurare a testelor de reziliență cibernetică TIBER-RO

Bank for International Settlements (2019), Report on open banking and application programming interfaces, November, https://www.bis.org/bcbs/publ/d486.pdf

Bank for International Settlements (2022), Business continuity planning at central banks during and after the pandemic, April, ISBN 978-92-9259-548-7, https://www.bis.org/publ/othp49.pdf

Bank for International Settlements (2022), Project Helvetia Phase II. Settling tokenized assets in wholesale CBDC, Juanuary, ISBN 978-92-9259-524-1, https://www.snb.ch/en/ mmr/reference/project_helvetia_phase_II_report/source/project_helvetia_phase_II_report.en.pdf

Balz, B. (2022), The impact of digitalisation on the financial system, April, https://www.bis.org/review/r220502b.pdf

Bălţoi, I.C.M., (2020), The fintech ecosystem in Romania, Proceedings of the International Conference on Business Excellence 14(1):273-281, July, https://www.research gate.net/ publication/343701831_The_fintech_ecosystem_in_Romania

Basel Committee on Banking Supervision (2022), Principles for the effective management and supervision of climate-related financial risks, Bank of International Settlements, June, https://www.bis.org/bcbs/publ/d532.pdf

Aysan, A.; Nanaeva, Z.; Shirazi, N.S. (2019). Open Banking from EU's Payment Services Directive to Practice: The Cases of Solarisbank and Insha, November, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3967612

Bianco, M.; Iride Vangelisti, M. (2022), Open Banking and Financial Inclusion, April, https://european-economy.eu/2022/open-banking-and-financial-inclusion/

Briones de Araluze, G. K.; Cassinello Plaza, N. (2023). Open banking: A bibliometric analysis-driven definition, October, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9529117/

Center for Internet Security, CIS Security Controls, https://www.cisecurity. org/

CIS Security Controls (Center for Internet Security), https://www.cisecurity.org/

Crisanto, J. C.; Prenio, J. (2020), Financial crime in times of Covid-19 – AML and cyber resilience measures, FSI Briefs No. 7, Bank for International Settlements, ISBN 978-92-9259-384-1

Crosignani, M.; Macchiavelli, M.; Silva, A. F. (2020), Pirates without Borders: The Propagation of Cyberattacks through Firms' Supply Chains, Federal Reserve Bank of New York staff report No 937

Dijmărescu, E.; Fugaru, A.; Curcă, S.; Oehler-Şincai, M.I. (2021). Transformarea monedei fiduciare, Academia Română, Institutul Naţional de Cercetări Economice "Costin C. Kiriţescu", Bucureşti, ISBN 978-973-159-269-5

Duffie, D. and J. Younger (2019), Cyber Runs, Hutchins Center Working Paper, 51

European Banking Authority (2019), *Action Plan on Sustainable Finance*, December, https://www.eba.europa.eu/sites/default/documents/files/document_library/EBA%20Action%20plan%20on%20sustainable%20finance.pd

European Central Bank (2022), Supervisory assessment of institutions' climaterelated and environmental risks disclosures, March,

https://www.bankingsupervision.europa.eu /ecb/pub/pdf/ssm.ECB_Report_on_climate_and_environmental _disclosures_202203~4ae33f2a70

European Commission (2020), Strategia de securitate cibernetică a UE pentru deceniul digital, Comunicare comună către Parlamentul European şi Consiliu, https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52020JC0018&from=ro

European Parliament European Council (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD 2), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri= CELEX:02015L2366-20151223

Florakis, C.; Louca, C.; Michaely, R.; Weber, M. (2020), Cybersecurity Risk, NBER Working Paper 28196

Greenberg, I., (2021), Fifth-generation cyberattacks are here. How can the IT industry adapt?, WEF, February 12.

Jamilov, R.; Rey, H.; Tahoun, A. (2021). The anatomy of cyber risk, NBER Workings Paper Series, Working Paper 28906, National Bureau of Economic Research, Cambridge, June, http://www. nber.org/papers/w28906

Khiaonarong, T.; Goh, T. (2020). Fintech and Payments Regulation: Analytical Framework, IMF Working Paper, WP/20/75

Klapper, L.; Lusardi, A.; Oudheusden, P. (2014), Financial Literacy Around the World: Insights from the Standard&Poor's Rating Services, Global Financial Literacy Survey

Kuo, C.; Lee, D.; Deng, R. H. (2018). Handbook of Blockchain, Digital Finance, and Inclusion, Volume 1. Cryptocurrency, FinTech, InsurTech and Regulation, Academic Press, London, ISBN 978-0-12-810441-5

Kuo, C.; Lee, D.; Deng, R. H. (2018). Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2. ChinaTech, Mobile Security,

and Distributed Ledger, Academic Press, London, ISBN 978-0-12-812282-2

Mersch, Y. (2019). Promoting innovation and integration in retail payments to achieve tangible benefits for people and businesses, Speech by Yves Mersch, Member of the Executive Board of the ECB, at the American European Community Association, Brussels, 7 February 2019, https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190207~f900d9105b.en.html

Miteva, A. (2022), 6 Types of Payment Fraud & How to Mitigate Them Effectively, January, https://www.mymoid.com/blog/types-of-payment-fraud/

Orr, A. (2022), The Future of Money demands innovation, February, A speech prepared for delivery to the Angel Association New Zealand Summit, https://www.bis.org/review/r220218b.pdf

Panetta, F. (2022), The digital euro and the evolution of the financial system, Introductory statement at the Committee on Economic and Monetary Affairs of the European Parliament, https://www.bis.org/review/r220616a.pdf

Parenti, R. (2020), Regulatory Sandboxes and Innovation Hubs for FinTech. Impact on innovation, financial stability and supervisory convergence, European Parliament, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, September, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652752/IPOL_STU(2020)652752_EN.pdf

Popa, A., (2021), Fintech startups and ecosystem trends in Romania, The Paypers, Insights into Payments and Beyond, July, https://thepaypers.com/expert-opinion/fintech-startups-and-ecosystem-trends-in-romania--1250735

Lane, T. (2021), Payments innovation beyond the pandemic, February, https://www.bankofcanada.ca/2021/02/payments-innovation-beyond-the-pandemic/

Rochemont, Sabrina, A Cashless Society - Benefits, Risks and Issues (2018). Issue 21- Environmental sustainability of a cashless society, Institute and Faculty of Actuaries, 2018, https://www.actuaries.org.uk/system/files/field/document/Issue%2021-%20Environmental%20Sustainability%20of%20a%20Cashless%20Society%20-%20disc.pdf

Shackleton, T. (2021), A Cost-Benefit Analysis Approach to Cyber Security, March, https://www.6dg.co.uk/blog/cost-benefit-approach-to-cyber-security/

Soderberg, G.; Bechara, M.; Bossu, W.; Che, N.; Kiff, J.; Lukonga, I.; Mancini-Griffoli, T.; Sun, T.; Yoshinaga, A., (2022), Behind the Scenes of Central Bank Digital Currency. Emerging Trends, Insights, and Policy Lessons, FinTech Notes, February

Terho, S., (2012), Către o piaţă europeană integrată a plăţilor efectuate cu cardul, pe internet şi de pe telefonul mobil (2012/2040(INI)), Comisia pentru afaceri economice şi monetare, https://www.europarl.europa.eu/doceo/document/A-7-2012-0304_RO.html

World Bank (2017), Principii aferente identificării pentru o dezvoltare durabilă: orientarea spre era digitală, Washington, D.C., World Bank Group

World Bank (2018). Romania catching-up regions. Raport final, https://documents1.worldbank.org/curated/en/784601580298213740/pdf/Romania-Catching-Up-Regions-Final-Report.pdf