Journal of Banking Regulation
https://doi.org/10.1057/s41261-024-00233-2

ORIGINAL ARTICLE

Legal implications of automated suspicious transaction monitoring: enhancing integrity of AI

Umut Turksen[1] · Vladlena Benson[2] · Bogdan Adamyk[2]

Accepted: 7 January 2024
© The Author(s) 2024

Abstract

The fast-paced advances of technology, including artificial intelligence (AI) and machine learning (ML), continue to create new opportunities for banks and other financial institutions. This study reveals the barriers to trust in AI by prudential banking supervisors (compliance with regulations). We conducted a qualitative study on the drivers for adoption of explainability technologies that increase transparency and understanding of complex algorithms (some of the underpinning legal principles in the proposed EU AI Act). By using human-centred and ethics-by-design methods coupled with interviews of the key stakeholders from Eastern European private and public banks and IT AI/ML developers, this research has identified the key challenges concerning the employment of AI algorithms. The results indicate a conflicting view of AI barriers whilst revealing the importance of AI/ML systems in banks, the growing willingness of banks to use such systems more widely, and the problematic aspects of implementing AI/ML systems related to their cost and economic efficiency. Keeping up with the complex regulation requirements comes at a significant cost to banks and financial firms. The focus of the empirical study, stakeholders in Ukraine, Estonia and Poland, was chosen because of the fact that there has been a sharp increase in the adoption of AI/ML models in this jurisdiction in the context of its war with Russia and the ensuing sanctions regime. While the "leapfrogging" AI/ML paths in each bank surveyed had its own drivers and challenges, these insights provide lessons for banks in other European jurisdictions. The analysis of four criminal cases brought against top banks and conclusions of the study indicate that the increase in predicate crimes for money laundering, constantly evolving sanctions regime along with the enhanced scrutiny and enforcement action against banks are hindering technology innovation and legal implications of using AI driven tools for compliance.

Keywords Artificial intelligence · Machine learning · Trust · Explainability · Transparency · Suspicious transactions · Anti-money laundering · Banking

JEL Classification G21 · G28 · K23 · O31

Introduction

The integration of artificial intelligence (AI) and machine learning (ML) systems in the banking sector has garnered considerable attention for its potential to enhance the efficiency and accuracy of anti-money laundering (AML) and combating the financing of terrorism (CFT) operations [1]. In this article, we delve into the legal implications of automated suspicious transaction monitoring, aiming to augment the integrity of AI systems in the banking industry.

To investigate this topic comprehensively, we employed a qualitative research design, interviewing senior managers from central and commercial banks and managers of IT companies developing AI/ML programs for banks. By comparing and analysing their responses, we gained valuable insights into the perspectives of bank managers regarding the utilisation of AI/ML systems. Our research findings shed light on the significance of AI/ML systems in banks and indicate a growing inclination among banks to embrace these technologies more deeply. However, during our exploration, we also encountered challenges in

✉ Umut Turksen
Umut.Turksen@coventry.ac.uk

[1] Centre for Financial and Corporate Integrity, Coventry University, Coventry CV1 2TU, UK

[2] Aston Business School, Aston University, Birmingham B4 7ET, UK

Published online: 06 February 2024

implementing AI/ML systems, primarily involving cost implications and economic efficiency considerations.

While AI/ML systems hold immense potential to optimise AML/CFT operations by rapidly processing large volumes of non-linear data, caution is warranted when implementing complex models [2]. The successful deployment of such models necessitates a well-coordinated team of highly skilled IT developers capable of promptly addressing any deviations in the functioning of AI systems. Furthermore, the availability of a well-structured and comprehensive database is paramount, as inadequate training data can lead to errors in the operation of AI/ML models. Overcoming these obstacles requires highly qualified data scientists with a profound understanding of the bank's operations, AML regulatory requirements, and the ability to swiftly reconfigure AI/ML models in response to operational changes.

For banks lacking the necessary resources and expertise, adopting more conservative approaches such as rule-based models may be preferable, as they offer greater control and transparency in system operations. Despite technological advancements, banks exercise caution when implementing complex AI models for AML/CFT activities, given the substantial potential costs of system errors regarding financial losses and reputational damage, as exemplified by selected case studies.

Moreover, explainability and transparency play pivotal roles in the practical application of AI/ML models in banks, particularly when regulatory authorities require a comprehensive understanding of the system’s actions.

Even with the challenges mentioned above, the widespread adoption of AI/ML models in banks and financial institutions (FIs) is increasingly imperative. While some banks actively embrace these technologies, others exercise caution. However, effective quality control of money laundering operations in the future will only be attainable by leveraging modern AI/ML models, particularly for large FIs.

Our empirical study provides insights into the drivers behind adopting AI tools in banking and highlights several factors that impede their widespread implementation. Moreover, our findings underscore the importance of understanding the ethical and legal standards of using AI/ML technologies in the banking sector. Promoting compliance and integrity within the industry is imperative to developing clear guidelines, fostering transparency, and enhancing the explainability of AI/ML models. By addressing these challenges and harnessing the potential of AI/ML, the banking sector can significantly enhance the effectiveness and efficiency of AML/CFT operations while ensuring adherence to legal and ethical standards.

The case studies examined in the article involve banks which were found guilty of failing to comply with AML/CFT standards and obligations. These cases are examined to highlight if and how AI/ML driven solutions could have mitigated risks.

The growth of AI/ML technologies in FIs poses four key questions:

1. Is the application of AI/ML in this domain trustworthy by prudential banking supervision requirements?
2. Can AI/ML programs be transparent and explainable to help end users understand critical financial decisions?
3. Can AI/ML models effectively meet global sustainability objectives while ensuring consumer rights and satisfying the growing users' appetite for sustainable investments?
4. What are the primary barriers inhibiting banks' widespread adoption of AI/ML systems, and how can these barriers be effectively addressed to promote the successful implementation of AI/ML technologies in banks?

The study findings will help inform banks' approach to harnessing AI technologies and legal and ethical requirements if they decide to do so. It ultimately will enable more harmonised practices and reduce the risk of criminal and civil penalties for banks.

This research contributes to the ongoing discourse on the intersection of AI and legal considerations in the banking industry, serving as a valuable resource for policymakers, regulators, and banking professionals seeking to navigate the evolving landscape of AI-driven transaction monitoring.

The paper is structured as follows. "Background to the topic" section reviews the key literature on the role of AI in Banking and regulatory approaches. "Methodology" section explains the methodology of the study. "Findings" section discusses the data analysis and findings. "Case studies: lessons from misuse of AI tools" section analyses case studies of banks’ non-compliance with AML/CFT standards. "Conclusions" section provides the conclusion.

Background to the topic

The increasing role of AI in banking and finance

Most European banks (over 90%) have been fined for AML-related offences in the past decade [3]. AI systems have emerged as indispensable tools to address the mounting challenges in handling substantial amounts of data. Nowadays, AI systems are increasingly used to assist in decision-making [4].

AI has a long history, reaching back to ancient Greece [5]. Its modern development can be attributed to Alan Turing and the 1956 Dartmouth College conference, where the term “Artificial Intelligence” was coined by John McCarthy [6] as “the science and engineering of making intelligent machines, especially intelligent computer programs” [7].

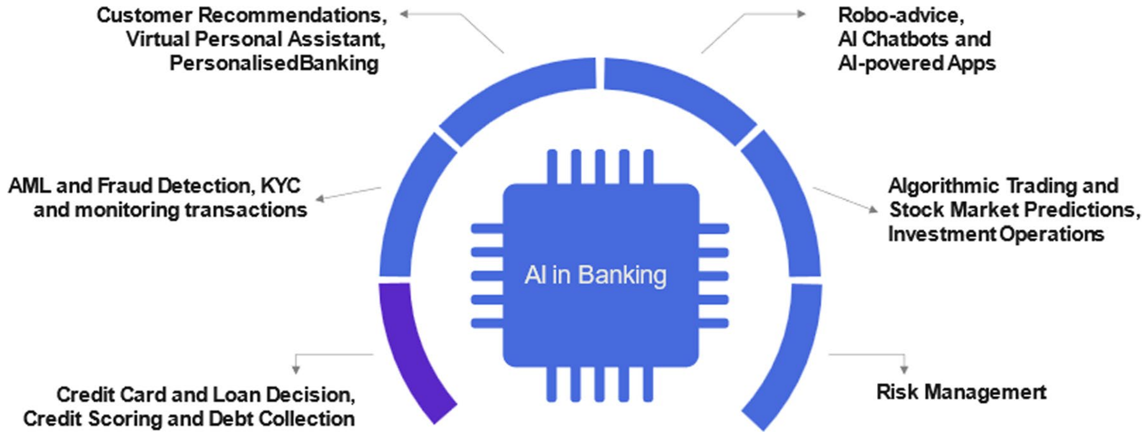
Customer Recommendations,
Virtual Personal Assistant,
PersonalisedBanking
Robo-advice,
AI Chatbots and
AI-povered Apps
AML and Fraud Detection, KYC
and monitoring transactions
AI in Banking
Algorithmic Trading and
Stock Market Predictions,
InvestmentOperations
Credit Card and Loan Decision,
Credit Scoring and Debt Collection
Risk Management

Fig. 1 Applications of artificial intelligence in the banking sector Source: Analysis of models by [24] and [25]

Nowadays, the term AI is often used to describe the project of creating systems with human-like intellectual capabilities, including reasoning, discovering meaning, generalising, and learning from experience [8].

A new wave of AI development emerged in the past decade due to ML algorithms. Machine learning is a subfield of AI, broadly defined as a machine's capability to imitate intelligent human behaviour [9] and as computational methods using experience to improve performance or to make accurate predictions [10]. ML was driven by access to vast data and the efficiency of graphics card processors for accelerating learning calculations [11]. ML differs from previous expert systems using an inductive approach, allowing computers to discover rules through correlation and classification using large datasets [12]. The objective is to understand data structure and automate tasks by integrating it into models.

Over the past 50 years, the concept of AI has evolved, and its application in various industries, including finance and banking, has become feasible due to advancements in data access, hardware capabilities, and sophisticated algorithms [13, 14].

The financial sector actively uses the capabilities of the AI system in its activities in various areas: data processing, robo-advice or chatbots, determining the creditworthiness of borrowers (assessment of the client's creditworthiness using various datasets), virtual assistants, trading robots, know your customer (KYC) processes, conducting customer due diligence (CDD), detecting fraud and market manipulation, monitoring transactions, credit scoring, algorithmic trading, loss and churn prediction, and debt collection (see Fig. 1). A key market where AI technologies are driving significant expansion is the Fintech industry. The 'AI in Fintech' market is expected to grow from $7.25 billion in 2021 to $24.17 billion in 2026 at a compound growth rate of 27.6% [15]. Explaining how machine learning algorithms arrive at decisions is indeed a challenging task [16]. Nevertheless, fulfilling this task is essential for humans to understand the AI solutions and develop trust in them [17]. The rapid pace at which the use of AI permeates does not align with the research conducted into the ways of securing it from adversarial threats. AI solutions that outperform human capabilities are becoming increasingly complex and unpredictable [18]. Therefore, if certain safeguards are not imbedded in AI-driven solutions, there exist significant risks that AI technologies could hinder the security, integrity, privacy, legal, ethical, and safety standards of financial systems [19].

AI systems significantly simplify and improve the quality-of-service delivery and are useful for both financial service providers and their customers. The De Nederlandsche Bank (DNB) expects further AI-driven innovations in various financial domains, ranging from leaner and faster operations ("doing the same thing better") to completely new value propositions ("doing something radically different") [20].

Development of AI systems responds to urgent market needs and therefore quality assurance is often an afterthought [21]. Investments in this technology and the complexity of AI system software continue to increase [22], shifting towards more and more complex AI models. The proliferation of AI systems gave rise to the problem of human trust in AI solutions [23].

On the other hand, the use of ML, a subset of AI, for prudential regulatory modelling, namely internal-ratings based (IRB) modelling, remains limited. FIs have been wary of using ML algorithms for calculating own funds requirements largely because of the challenges associated with model interpretability [26].

More recently, ML methods and, to some extent, deep learning (DL) have been used by regulators to assess credit risk and predict bank failures [27]. Currently, traditional statistical methods are still widely used for this purpose. Nevertheless, ML techniques outperform traditional approaches by allowing practitioners to model past decisions, exploit them for other scenarios, and predict future chaotic phenomena [27].

FIs are required by law to have in place an effective, risk-based Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) framework, which includes the application of a risk-based approach to CDD measures, reporting of suspicious transactions, governance, policies and procedures, record keeping and training [28]. These standards are necessary as the huge amount of dirty money from criminal activities such as drug trafficking and money laundering continues to pervade and blemish the global financial system [29]. Financial criminals, such as money launderers with advanced and sophisticated capabilities, tend to outwit the current capabilities of law enforcement agencies (LEAs) as well as the effectiveness and efficiency of AML legal and regulatory frameworks [30].

Several AML scandals have pervaded the global financial system for which a number of high-profile banks have been and are being investigated and prosecuted by regulators and LEAs globally for their apparent failure to stop their institutions from being used as a platform for laundering illicit funds. FIs that lack compliance and due diligence were already fined $2.7 billion in 2021, according to AML Fines 2021 Report [31]. While the total amount of AML fines fell from $3.2 billion in 2020 to $2.7 billion in 2021, the number of FIs fined has increased—from 24 in 2020 to 80 in 2021. The following provisions highlight some of the significant scandals and how AI could have been applied in legal contexts.

The dilemma that banks are using AI/ML in compliance but are still receiving fines for non-compliance with AML regulations can be reconciled by considering three main challenges: the complexity of regulations; data quality; transparency and explainability [1].

Financial regulations are complex and ever-changing. Banks must comply with various laws and regulations, such as AML, KYC, and consumer protection rules. AI can assist in automating compliance processes and detecting suspicious activities, but ensuring full compliance requires a deep understanding of complex regulations, which may surpass current AI systems' capabilities.

AI/ML algorithms heavily rely on data for training and decision-making. Banks may face challenges obtaining high-quality, well-labelled training data, especially for compliance-related tasks. Inadequate or biased data can lead to flawed AI/ML models, which may not effectively address compliance requirements [25]. Additionally, certain types of data, such as unstructured data from legal documents or regulatory updates, may not be readily available or efficiently utilised by AI systems.

Compliance regulations often require transparency and explainability to demonstrate how decisions are made. Banks need to justify their compliance decisions to regulators, auditors, and customers. Many AI models, such as deep learning neural networks, can be complex and challenging to interpret [32]. While efforts are being made to develop explainable AI techniques, there is still ongoing research to improve the interpretability of complex AI models and make them more suitable for compliance purposes. Banks must also continuously adapt their AI systems to address emerging risks and vulnerabilities, which can be challenging and ongoing.

To bridge the gap and enhance the current use of AI, we aim to identify the critical challenges concerning employing AI/ML algorithms in banks by interviewing senior managers and conducting doctrinal legal research by analysing law and court cases.

Banking regulators must have confidence that the AI systems based on which managers make decisions for FIs are fair, robust, explainable, accountable, and aligned with the values of society and the regulatory framework they are designed for [33]. Regulators of various countries are actively developing a new regulatory framework to combine efficiency for developing the financial sector and the protection necessary to minimise customer risks [34].

Another challenge for regulators of FIs is the rapid development of fintech start-ups that provide financial and non-financial services in the supply chain and actively use AI systems. An appropriate legal field has been created for banks, and banks have considerable experience, relevant departments to ensure compliance with the banking legislation. The banks also have experience in the field of AML control [35]. Banks try to adhere to the AML legal instruments as non-compliance penalties can be severe. Typically, banks thoroughly test and audit the AI systems they use because they understand the risks involved to minimise commercial and reputational risks [36].

Unlike well-established banks, new fintech companies do not have the level of experience and in-house capability to control financial transactions. Many new fintech companies fail to meet the rigorous approach to AML/CFT requirements [1]. It has been shown that shortcomings in the due diligence and know-your-customer systems (sometimes they do not perform customer identification at all) occur at the fintech start-up level [37]. Accordingly, when choosing AI systems, compliance with legal obligations (e.g., AML/CFT, fraud prevention, etc.) as an inherent element of the operations is not always a priority, especially for companies operating in the field of decentralised finance and crypto assets [38].

AI in prudential banking

According to the report by the Bank of England (BoE) and Financial Conduct Authority (FCA) survey of the banking and finance sector (including banks, trading platforms, and fund managers), 66 per cent were employing ML and often in several areas of their operations [39]. Data shows that ML is increasingly used in both front- and back-office settings, fraud prevention, AML, and customer service settings. Until recently, AI/ML programs were used mostly by hedge funds and high-frequency trading companies [40]. However, many firms are now deploying AI/ML more broadly, with the most prominent in the banking and insurance spheres. Central banks of different European countries actively embedded AI into their daily operations, from micro-prudential and macroprudential supervision to information management, forecasting and detecting fraudulent activities [41].

Inappropriate use of AI systems in Banking and Finance can cause significant damage not only to business stability and profitability but also to customers. This highlights the ethical and legal issues and the need for the evolvement of existing regulatory regimes of FIs, considering the current and future risks caused by the use of AI systems [42].

AI systems are used not only by commercial banks and the private financial sector. Central banks also assessed the advantages of using AI in various areas of their activities, particularly in monetary policy, handling data collection and policy forecasting. AI can improve the information flow to the monetary policy committees at a much lower cost than with current infrastructure. Such AI systems in micro-prudential regulation reduce costs, increase efficiency, help with crisis response, and can be highly resilient (operating 999 out of 1000 days) [43].

The effectiveness of AI systems in macroprudential regulation is yet to be fully understood. Firstly, the active use of AI systems can cause procyclicality and increase systemic risks [44]. Due to the fact that AI systems perceive and process new information in the market in a standardised way, all FIs can make an instant decision to buy/sell the same assets [2]. The problem for AI systems is processing new events that did not exist before (unknown-unknown) such as the COVID-19 pandemic, economic crises, wars, etc. Predicting the results and efficiency of AI systems in such events is quite difficult. AI models work in infinitely complex environments and can have unexpected behaviours or nodes of information fed to them. AI models with fixed objectives can run into cases where they take critical decisions like no human would [45]. Humans can adjust their objectives in light of complex factors that may emanate from social, legal, political and environmental ecosystems. AI models cannot do so without human input and can only facilitate optimisation against the system.[1] Hence, meaningful human control must be a key component of all AI systems.

The legal framework envisaged for the use of AI in Europe

The EU Commission in 2021 published the proposed law (EU AI Act 2021)[2] for laying down the standards on AI, with the intention of putting forward legislation for a coordinated approach on the human rights and ethical implications of AI [46]. This is the first legislative framework on AI that has been put forward by the EU and has the potential to "set the tone" internationally and particularly for the states who are candidates for EU membership. The EU AI Regulation is not only novel, but it is also a comprehensive framework unlike other EU legal instruments which only refer to AI in passing and do not holistically introduce 'risk-management' considerations for AI systems. Just like the General Data Protection Regulation (GDPR) 2016 and AML, the proposed AI regulations is also underpinned by a risk-based approach. In the first instance, an essential step is to use risk and risk management tools as a means to better comply with the GDPR 2016. Secondly, it is essential to determine which and how AI systems should be regulated.

The proposed EU AI Regulation requires a risk-based approach to the use of AI technology whereby high-risk AI systems would be subjected to stricter safeguards.[3] Article 5

[1] AI models with fixed objectives require human intervention or guidance to perform their tasks effectively. They are designed for specific tasks or goals with predetermined and predefined objectives. These AI models include supervised learning models and reinforcement learning models. Human involvement remains vital to these AI models' training, fine-tuning, and overall functioning. Unsupervised machine learning models do not require direct human input during the training phase. They still require human intervention in certain aspects. Unsupervised models learn patterns and structures from unlabelled data without human-labelled examples. However, their performance and usefulness often depend on human involvement in the pre-processing and interpretation stages.

[2] Proposal for a Regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union Legislative Acts, COM/2021/206 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206.

[3] The proposed AI Regulation contains specific rules for AI systems that create a high risk to the health and safety or fundamental rights of natural persons. High-risk AI systems are permitted on the European market subject to compliance with certain mandatory requirements and an ex-ante conformity assessment. The classification of an AI system as high-risk is based on the intended purpose of the AI system, in line with existing product safety legislation. Therefore, the classification as high-risk does not only depend on the function performed by the AI system, but also on the specific purpose and modalities for which that system is used. The European Commission describes these systems as "limited risk" systems, but this description is not explicit in the regulation. See, https://www.europarl.europa.eu/

of the proposed AI Regulation deems certain types of social scoring and biometric surveillance to be an "unacceptable" risk to privacy, non-discrimination, and other related human rights, thus bans such AI systems completely ("Case studies: lessons from misuse of AI tools" section of the Explanatory Memorandum) [46].

Public authorities are prohibited from scoring people's "trustworthiness" in one aspect of their lives (e.g., their ability to repay debt) to justify "detrimental or unfavourable treatment" in another, unrelated context (e.g., denying them the right to travel). In the opinion of the authors of this paper, the current proposal to ban some types of "trustworthiness" scoring over a "certain period of time" is vague and impossible to implement meaningfully (Article 5) [46]. Instead, the regulation should prohibit any type of behavioural scoring that unduly restricts or has a negative impact on fundamental human rights such as privacy and non-discrimination. In regard to the use of AI tools by banks, the hypothetical scoring systems that would try to predict whether customers are a fraud risk based on KYC records or serve as a pretext for acceptance or denial of an application, should be banned if it conflicts with an applicant's fundamental human rights, including privacy and non-discrimination.

The EU's proposed AI Regulation requires each AI system to be classified in terms of the risks such AI may pose to society. In our opinion, the category of the AI system proposed for due diligence and processing customer data in banking services would be categorised as a "high-risk" AI system as it would handle and analyse personal/customer information which would in turn contribute towards determining whether customers would be entitled to various services or benefits [47]. The AI tools that interact with customers about services and products (e.g., a chatbot) on the hand would be a low-risk AI system.

Importantly, the proposed AI Regulation designates an expansive list of AI systems as "high-risk" that would require extra safeguards to deploy. More specifically, these systems include those used to identify and categorise people based on their biometric data, such as facilitating a minimum KYC due diligence standard in banking services [46].

AI use cases in facilitating minimum standards would have to meet certain "high-risk" requirements under this proposed regulation, which could be deemed as onerous. Therefore, as the use of AI in risk analysis and AML compliance offers many opportunities, it offers, equally, many challenges. The vast amount of data available to banks empowers advanced decision-making, but in tandem also raises questions pertaining to the quality of the datasets and how these are utilised. Provisions of the proposed AI Regulation require that the datasets used in creating an AI system must be free of errors [48]. The AI Regulation also sets harmonised rules for the development and placement on the market as well as use of AI systems in the EU following a proportionate risk-based approach. It can be recommended, therefore, that the placement of AI facilitating minimum due diligence standards in the banking industry, shall also take a proportionate risk-based approach. It is important that an AI system in banking follows predictable, proportionate, and clear obligations, which are also placed on providers and users of those systems to ensure safety and respect of existing legislation, protecting fundamental rights throughout the whole AI systems' lifecycle.

This is a model which should be followed by banks for all intents and purposes. The legal requirements for a high-risk AI system in the banking sector, in relation to data and data governance, documentation and record keeping, transparency, human oversight, robustness, accuracy and security, must be clear. Article 10(2) of the proposed EU AI Act stipulates that organisations with high-risk AI systems, such as financial services providers, shall make use of training of data models and validation and testing of datasets [49]. In addition, such organisations shall take proactive steps to outline relevant design choices and examine possible data biases that may lead to the risk of cyber-security vulnerabilities. For example, Article 14 requires that developers and users of high-risk AI systems conduct periodic human oversight of such AI systems. Failure to adhere to such requirements may attract a regulation fine amounting to € 30,000,000 or 6% of the company's annual turnover during the preceding financial year.[4] Therefore, it can be argued that the sanctions regime under the new AI regulatory framework is more stringent than the one under the GDPR framework.

The above summary of legal requirements for adopting AI tools sets the compliance benchmarks that the banks shall consider in adopting AI/ML driven services.

Methodology

Research design of the study

To address our research questions, we applied doctrinal legal research by analysing law and court cases and a qualitative research approach by means of a series of semi-structured interviews.

This research is conducted among banks' senior managers, who are responsible for AI/ML systems in their banks. 12 respondents who directly make decisions in the field of

Footnote 3 (continued)

news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence.

[4] Article 71 of the Draft EU AI Act.

application of AI/ML systems were selected. The respondents include 7 managers of Ukrainian banks with different forms of ownership, 2 managers of the central bank and 3 managers of IT companies (Estonia, Poland, Ukraine) specialising in the development of AI/ML systems for banks in Ukraine and in other European countries. In order to ensure the anonymity of banks and respondents, we applied the following coding system. For respondents from commercial bank—B1, B2, B3, B4, B5, B6, B7; for respondents from the central bank—C1, C2; for respondents in the fintech solutions category– S1, S2, S3.

All banks are among the 20 largest banks in Ukraine by capital size. The first three banks (B1, B2, B3) are banks with state capital, all of them are among the top 10 largest banks of Ukraine, and the number of clients of these banks exceeds 10 million people. Banks B4, B5, B6, B7 are banks with private capital. The number of their customers exceeds 2 million people. Bank B4 is a bank with foreign private capital. Banks B5, B6 and B7 are banks with Ukrainian private capital. Thus, we covered all groups of banks of Ukraine by form of ownership.

The choice of Ukrainian banks as a use case of using AI systems is related to the fact that the banking system of Ukraine is integrated into the international payment space and technologically works according to the same standards as the leading countries of the European Union, Great Britain and the USA. Furthermore, given the ongoing war in Ukraine, the due diligence, AML/CFT, fraud detection capabilities have become even more important. Ukraine plans to become a full member of the European Union as soon as possible (Ukraine has been an associate member of the EU since 2022). Moreover, the level of technical and software support of banking operations that Ukrainian banks consider, the standards and principles of Ukrainian banks' activities regarding the control of operations related to money laundering and the fight against terrorism, are of great importance and are poorly researched. The findings then are compared across the recent criminal cases brought against banks, and propositions are made based on empirical evidence.

Data collection

Data collection was carried out between September and October 2022. To keep validity and completeness of the data, main principles of data collection were followed: using various sources of information, building a case study database, and preserving the chain of evidence.

All interviews were attended by senior managers of banks who were directly involved in the work of AI/ML systems and performed a supervising/governing role. Some interviews (4 from 12) had experts with technical expertise directly involved in developing the AI/ML systems. Each interview lasted from 1 to 1.5 h. A total of 12 interviews were conducted. All these interviews were recorded, and transcripts were prepared, which were then confirmed by the interviewees.

The top management of the banks and FIs were asked questions regarding: the context of how and where AI/ML models are used; challenges regarding the internal user acceptance of AI/ML models; questions about transparency, level of accuracy, liability and consumer protection rules, accountability and ethics practices, interpretability, oversight mechanisms, interpretability with the different stakeholders, safety risks, system's auditability, level of explainability, and potential financial liabilities. Finally, we discussed the barriers affecting the adoption of AI/ML by banks and FIs and the perspectives of supervisory authorities regarding the application of AI/ML.

Data analysis

Data analysis was conducted based on the interview transcripts. As a first step, we analysed the interview reports and created a list of the key themes per interview. These findings and conclusions were verified by the interviewees. As a next step, we analysed all interview reports and the coding scheme was applied. The results of the thematic analysis were discussed in a plenary session with and expert panel participants of the supervisory authorities, banks and IT companies. The feedback from this panel was used to refine the conclusions.

Findings

In this section we discuss the data analysis findings.

Perspectives of supervisory authorities and regulated entities regarding the application of AI/ML in prudential supervision

Almost all respondents noted that the main goal of the business strategy of modern banks is the digitalisation of services and the creation of financial ecosystems. The vast majority of banks use AI/ML systems in their day-to-day activity, and many banks use these systems in several divisions to solve different tasks.

The regulator's requirements for AI/ML systems exist and are prescribed in regulatory documents, but usually, they are general and relate to various areas of activity of the company. For example, in the field of AML, prudential regulation, risk analysis, monetary policy, statistics, finance, cash flow, etc. In Ukraine, prudential and AML/CFT supervision of banks and other FIs is provided by the same national body—the National Bank of Ukraine (NBU).

The respondent from the central bank C1 emphasised that the NBU has adopted a proactive approach to supporting the development and implementation of AI/ML in the prudential supervision of Ukrainian banks. As a regulator, the NBU has acknowledged the potential benefits of AI/ML in enhancing the efficiency and effectiveness of supervisory processes, strengthening risk management practices, and improving the accuracy of risk identification and assessment. To this end, the NBU has developed guidelines for using AI/ML in financial institutions that include transparency, accountability, and data protection requirements [50].

Many central banks have formulated a distinct strategy to facilitate the advancement of Supervisory technologies (SupTech) and Regulatory technologies (RegTech) [51]. The principal objective of regulatory authorities concerning the implementation of SupTech and the promotion of RegTech development is to establish an innovative, proactive, and technologically-advanced regulatory framework, which is grounded in a robust technological infrastructure, digital expertise, and a comprehensive reassessment of the regulatory and supervisory procedures themselves [52]. Through the implementation of RegTech, banks can optimise their compliance with regulatory requirements, while the regulators, in turn, can leverage SupTech to automate and streamline supervisory processes. The overarching aim is to support cultivating a resilient, well-governed, and competitive financial sector by effectuating a paradigm shift in the supervisory process by incorporating advanced technological tools and techniques.

From the point of view of the representative of the central bank C2, there is great interest in using AI/ML models by banks, as the growth of the role of high-frequency data is significant. Implementing AI/ML solutions hinges on using high-quality data characterised by reliability, timeliness, structuredness, and machine-readability. Since data analysis forms the basis of decision-making processes, ensuring data quality is paramount.

The central bank uses all of these in prudential regulation and macroeconomic analysis. However, it is pretty challenging to draw a parallel between the use of complex AI/ML models and the need to decompose them into a traditional understanding of the relationships between shocks and reactions, which would be optimal for the central bank.

The respondent from the central bank C2 also noted that the NBU is cognizant of the potential risks associated with using AI/ML in prudential supervision. These risks include the introduction of biases and the possibility of models producing inaccurate results. To mitigate these risks, the NBU has emphasised the importance of implementing robust governance frameworks and conducting comprehensive testing and validation of AI/ML models.

The central bank also uses AI/ML systems in its internal activities, particularly in prudential regulation. AI/ML programs are used in many support services by different central bank departments. These are the so-called supporting programs, with the help of which it is possible to analyse an array of data and make appropriate decisions. Thus, the effectiveness of the central bank's work in prudential regulation increases.

Based on the results of the interviews, we can assume that regulators in Ukraine maintain a technology-neutral stance. It implies that they promote the development and utilisation of AI/ML solutions by banks without mandating or forbidding the use of specific AI/ML technologies.

Bank respondents divided the regulator's requirements for AI systems into two blocks. The first block of requirements concerns areas of activity related to financial monitoring and risk management ("block of risks"). In this block, the regulator has clear requirements for the interpretation of AI/ML models, as well as the entire flow, pipeline and model validation. These requirements of the regulator are followed very strictly. The compliance team constantly monitors this. All models that the banks create and use in the "block of risks" must fully comply with the regulator's requirements, as banks are well aware that otherwise, the fines will be quite significant. Supervisory authorities periodically conduct audits on the compliance of AI programs with current requirements. Everything related to risks is under the watchful control of the regulator.

For example, suppose it concerns AI/ML programs used by Bank 2 for operations not related to risk and reporting, such as recognising the customer's face through the use of computer vision technologies, to search for criminals or identify unscrupulous customers who are trying to get a loan from the bank using forged documents. In that case, there are no regulatory requirements regarding such types of operations and the use of AI/ML programs. Bank 2 uses its internal team approaches from the developer's point of view, particularly the model lifecycle, monitoring, data quality, interpretability of results, etc. Such AI/ML systems are more focused on the bank's needs and have no regulatory requirements.

Regarding the models that banks use for financial monitoring, banks generally do not use complicated ML algorithms and advanced AI models in this area. For example, graph databases are used to build relationships between counterparties, logistic regressions are used as well. There are certain algorithms (mostly rule-based models) for determining the relationships between counterparties, which allows to successfully search for suspicious transactions, missing which the bank can potentially receive fines. The main reason why banks do not use more complex AI/ML systems is frequent changes in legislation and regulatory requirements. Therefore, the banks consider using rule-based programs and simple algorithms in this area more expedient, which the bank's IT employees can quite easily change.

All surveyed Ukrainian banks have sufficient internal personnel to handle the flow of risky transactions. The main task of the AI/ML programs is to help bank staff make better decisions based on notifications about suspicious transactions. For this, some banks often use graph technologies to make it easier for an employee to visualise the chain of transactions.

Software developers are also cautious about using complex AI/ML models in transaction monitoring. The representative of the software development company considers it more appropriate to use not AI/ML programs in the field of financial monitoring but what they call "augmented intelligence" programs. These programs focus on a limited number of intelligent tasks and support humans in decision-making. It is not AI driven by computers. It is insights generated from algorithms from machines, from processes put in place complemented with human insights. It is machine intelligence augmented with human intelligence. Many AI/ML models will run into trouble with supervisory authorities if they are deemed inadequate in preventing bias, so it is critically important to have human insights and meaningful human control in the AI/ML models.

From the point of view of the central bank representative, there is great interest in the use of AI/ML models by banks, as the growth of the role of high-frequency data is significant. The central bank uses all of these in prudential regulation and macroeconomic analysis. The NBU also uses AI/ML systems in its internal activities, particularly in prudential regulation. AI/ML programs are used in many support services by different central bank departments. These are the so-called supporting programs, with the help of which it is possible to analyse an array of data and make appropriate decisions. Thus, the effectiveness of the central bank's work in the area of prudential regulation increases.

The role of transparency and explainability of AI/ML models

For financial institutions, especially from the point of view of regulators, transparency and explainability of AI systems have an essential value. Modern AI systems are complex and use more and more powerful algorithms, and as a result, they are more accurate. At the same time, they are usually less transparent and explainable, which is more costly for oversight. These two principles are closely linked, but they have separate meanings.

One of the definitions of 'Transparency' is that 'transparency' relates to designing and building AI systems so that there can be effective oversight [53]. A primary element of transparency is a clear understanding of each input data elements' importance in connection to the accuracy of the output prediction. Banks and other FIs should be able to describe the data and features used, the mechanisms by which outputs are generated and how decisions are made.

Businesses should consider explainability as a means to promote trust with customers, regulators, auditors and other stakeholders (trust in FIs is highly important). The crucial role of trust in the financial sector is considered necessary explainability of the outcomes and functioning of AI systems [54].

'Explainability' can be interpreted differently but broadly means that an explanation of a system's operation and outcome can be formulated so the stakeholder can sufficiently understand it [55]. AI solutions utilise data (e.g., on an individual's financial situation) and produce an outcome (e.g., rejecting a certain loan). However, there is generally no output in this process that explains how or why the outcome is reached based on the data. Especially in the case of AI techniques such as deep neural networks, the process from input to output is virtually impossible to interpret, even with knowledge of the system's inner workings, weights, and biases. XAI explains why or how the AI solution arrived at a specific decision [56]. It refers to taking the technical elements of the AI system (often referred to as "opening the black box")[5] and providing a 'translated' explanation (in the form of details, reasons, or underlying causes) that is understandable and comprehensible to human beings [53]. An improved understanding of how these algorithms work helps us verify, improve, and implement them ethically [57].

By clarifying how AI systems operate, transparency and explainability can help firms more easily satisfy other criteria for trustworthy AI, such as fairness, managing bias and ensuring accountability [53].

Financial institutions use AI/ML programs in areas with a significant flow of incoming information that needs to be analysed. Employees are generally optimistic about the implementation of AI/ML systems, particularly in the field of transaction monitoring and AML operations. On the one hand, the introduction of new AI/ML programs implies a reduction in the number of employees in certain bank departments. However, on the other hand, the employee understands that monitoring transactions with AI/ML programs is much more effective. Therefore, such programs help employees in their work and reduce the probability of

[5] In AI, a "black box" refers to an AI/ML algorithm whose internal workings or decision-making processes are opaque or not easily explainable to humans. It means that while the inputs and outputs of the system are observable, the internal mechanisms and logic used by the AI system to arrive at its decisions are not transparent or understandable. The "black box" nature of AI systems can make it challenging for regulators, users, or stakeholders to comprehend how the system arrived at a particular outcome or decision, raising concerns about accountability, fairness, and potential biases. See: [58].

skipping certain operations if they were to be carried out manually. The financial responsibility lies with the bank and, accordingly, with the employee as well. Therefore, the employees who control AML/CFT operations are usually very positive about implementing AI and machine learning systems, provided they understand how the system works and how effectively it monitors transactions.

The respondent from the software company noted that the model's accuracy is paramount when developing an AI/ML model. Developers evaluate model results on "out of time" samples, validation samples, and the model's stability are assessed. Data samples are taken as representative, as usual a significant percentage of the client base (sometimes 5–20%) is taken. Sampling is carried out by randomising the incoming flow of customers. If the bank has several million customers, then for a sample of even 1 million, there will be a good distribution of customers in various categories.

However, there are various tasks of what level and definition of accuracy would be required in the context of the AI/ML system and different use cases. For example, there are tasks where ML approaches are used in data classification (data management processes) and processes for maintaining the data catalogue in an up-to-date state. There are also data discovery pipeline processes. In some AI/ML models, it is established that the accuracy of choosing data should not be lower than 90%. Everything below is manually classified by the bank employee. These are quite strict rules and usually they concern the areas of risk management and financial monitoring.

The indicative accuracy parameter is less important for AI/ML models related to the bank's internal business processes, particularly customer service, provision of certain services, and attracting new customers. Accuracy is not always the most important factor when deciding on implementing such a model. Sometimes the bank is ready to go on a "sandbox" experiment,[6] implements this AI/ML model, and the model is tested on a small segment of customers. The process of improving the model is taking place and the bank understands how effective this model is from the point of view of the bank's business goals and whether it is expedient to implement this model for the entire client base of the bank.

Thus, depending on the scope of application and the set tasks of the AI/ML model, the value of the model's accuracy during its implementation is different. However, any AI/ML model has to have transparency across the lifecycle of the model. It is one of the most important parts. Many AI/ML initiatives can be accused of being a "black box" [58]. After they get some elaborate computations, the model developer puts all the data in and then spits out a bunch of results. It is crucial for developers that those individual results can be executed especially by end users. For example, when testing the fraud model and comparing it with historical data, they can see a 15% improvement, and they must understand where that improvement has come from and what the outcomes are now. That is a critical part of the process, especially for transaction monitoring.

The question of explainability of AI/ML systems does not have an unequivocal answer. The AI field is very diverse. Therefore, the answers of the respondents differed. All experts agreed that for AI/ML models that monitor transactions, one of their tasks is maximum explainability, since the employee works with the model's solution directly in the future. Further effective decision-making by the employee depends on the employee's understanding of the criteria according to which the model selected a risky operation. For example, the models include an algorithm that allows the employee to directly see the reasons why the model assigned a certain operation to the risk category. This makes it easier for the employee to make the correct final decision.

Therefore, explainability is of great importance in AI/ML risk models and is given maximum attention. Scientists reveal the logic of the model's operation. When discussing the results, the manner in which the results were obtained are explained in the maximum detail. In addition, the operation of AI/ML risk systems is constantly monitored to prevent the occurrence of false results.

As for the AI/ML models that serve the bank's business tasks, for example, choosing the best offer on the market, choosing the best communication channel, etc., there are no specific requirements for the explainability of the models. The models are so complex that not all models require worker-level explainability in practice. Usually, the requirements for explainability of the model are put forward at the beginning of its creation and development. IT developers are trying to understand how exactly the AI/ML model will be used in banking processes, whether this model needs explainability and to what extent it is needed. For example, based on the task, model developers may decide that the model should be as transparent as possible (so that they can build a model with a simple algorithm based on linear regression).

Sometimes, stakeholders do not need a detailed interpretation of certain business processes and tasks. Therefore, in such AI models, more complex algorithms are used, without a detailed explanation to all users of the model due to which factors the model produced the result. The model user

[6] "Sandbox" (in the context of AI) is an environment or framework that allows for the testing and experimentation of new AI technologies in a controlled and supervised manner. It provides a safe space where innovators, developers, or companies can pilot and evaluate their AI products or services while being subject to certain regulatory constraints. The purpose of a sandbox is to strike a balance between encouraging innovation and ensuring compliance with existing regulations. See: [2].

receives general information, for example, which variable has a greater specific weight and which is less. That is, the employee has a general understanding of the result obtained. Nevertheless, it is difficult and unnecessary to explain in detail the entire depth of connections and solutions of the model in certain areas.

Respondents agreed that AI/ML models are part of the complex banking process. Adjustments to model results often occur. In some cases, the model is improved, in others, expert rules work, where a person makes the decision. Everything is documented, an appropriate transparent algorithm is prescribed, and certain decisions in complex processes are made both by machines and by humans. At the same time, all processes at the database level are saved, so that later it is possible to conduct a retrospection and understand which cascade of decisions the process went through before the result was obtained. It also underpins the principles of accountability, traceability, and transparency.

Global sustainability objectives and consumer-friendly approach: Do AI/ML models meet them?

All respondents indicated that their FIs seriously consider liability and consumer protection rules. The protection of consumer rights and the protection of databases are given considerable attention when developing and using AI/ML systems. It is not only due to legal requirements, possible lawsuits from customers and, as a result, fines. The reputation of the bank is of great importance. Not paying due attention to these issues carries a significant reputational risk for the bank.

A representative of a large bank with state capital (Bank 1) noted that there were some cases when clients complained about the results obtained as a result of AI/ML systems' solutions. Mostly, such cases were related to individual customers in the field of consumer credits, setting credit limits, etc. and were not related to financial monitoring. Banks respond to customer complaints by considering the cause of the complaint in detail and try, sometimes in semi-manual mode, to correct the error in the AI/ML system. Bank 1 always has a "plan B", when the bank's management realises that the AI/ML model can make a mistake, or there may be problems with the incoming data stream that were not taken into account in the process of filtering, cleaning the data and checking its quality. The presence of "plan B" allows Bank 1, when a problem is detected, to roll back the system and make the correct decision or overwrite the correct decision in the system. These are back-office processes; quite a few allow processing specific problem solutions in automatic or semi-automatic mode.

We can assume that human experts play a vital role in reviewing and verifying the outputs generated by AI algorithms, particularly in complex or "high-stakes" scenarios. While AI can automate various tasks and processes, it is essential to have checks and balances in place to identify and rectify any errors or inaccuracies that may occur. This human-checking process acts as a corrective mechanism to catch and correct any mistakes AI systems make, ensuring the integrity and quality of the bank's operations. It highlights the significance of human oversight and validation in ensuring the accuracy and reliability of AI systems, not just for consumer data but also for other critical functions within the bank, including compliance.

More and more often, banks give priority to the issue of environmental protection. They establish mechanisms to measure the environmental impact of the AI/ML system's development, deployment and use. One of the analysed banks (Bank 3) states in its strategy and all advertising campaigns that the bank is "environmentally green". When developing AI/ML models, attention is paid to systems' ecology and energy consumption. Bank 3 tries to carry out paperless activities as much as possible and minimise the printing of contracts, checks, etc. The task is to minimise paper document circulation, whereby all documents are available in digital channels, and the bank client has access to electronic confirmation immediately after carrying out a certain operation. For a bank with tens of millions of customers, implementing paperless technologies is of great importance.

The efficiency of energy consumption is also an important priority. Some banks (Bank 2, Bank 3 and Bank 5) have moved part of their operations and databases to the cloud, so the issue of energy consumption efficiency is not their top priority in that part. However, when developing AI/ML systems, banks primarily look at cost performance parameters. It should be really effective from the point of view of the cost of computer and energy resources and, in general, the cost of infrastructure in all processes should be minimal.

Consumer data protection is a priority for banks when developing AI systems. There were many cases of theft of bank customer databases and cases of database sales in previous years in Ukraine. Some banks were fined for inadequate control. This issue is receiving considerable attention nowadays. Legislation in this area has improved, and there are clear rules that banks must follow. The presence of clear rules obliges banks to treat customers' data at the appropriate level at all stages of the development and operation of AI/ML systems.

Each bank pays considerable attention to ethical issues at all activity levels, including AI/ML models. This direction is given a significant role. Compliance departments operate in each bank. Rules are prescribed, meetings and training are constantly held. These things are controlled thoroughly, and the penalties are severe when certain violations are detected.

All respondents agreed that their banks and financial companies are aware of the potential financial liabilities in case AI/ML systems fail compliance. Everyone clearly understands that it is a fine if the system misses any risky payment. If something is not done correctly, it is a fine as well. Penalties for violating the legislation in the field of money laundering and financing of terrorism are significant and can reach in Ukraine, for example, up to 1% of the authorised capital of the bank. For big banks, this can reach hundreds of millions of euros.

Therefore, when designing a pipeline of the AI model, banks always have different scenarios with a possibility for a certain work around. There are anomaly assessment systems that allow minimising potential threats to the bank. It is essential for developers of AI systems to understand whether there are certain anomalies from the standard behaviour of the system. If this is found, appropriate decisions are made immediately.

All respondents noted that banks' work on meeting the international AML/CFT standards (e.g., FATF Recommendations) and other legal requirements (e.g., EU AML Directive) is highly important. Financial monitoring issues are controlled by banks very carefully.

Measures to enable audit and to remedy issues related to governing AI/ML autonomy

Monitoring and testing of AI/ML systems to ensure they meet goals, purposes and intended applications are permanent. The system of monitoring is an integral component of the life cycle of any AI/ML model. Any deviations in work are corrected as quickly as possible. Not only testing, but also improvement of systems is constantly underway. Some changes need to be made constantly, for example when regulatory requirements change.

All respondents indicated that the banks had established oversight mechanisms for data collection, storage, processing and use. They noted that the banks have appropriate internal monitoring systems. Quality metrics of the model's performance, appropriate dashboards and alert systems exist. A team of scientists monitors these metrics continuously. In addition, there are rules in the bank to reconfigure the AI model once a quarter or once a half year. New features may appear, and previous ones may not be relevant. Banks have technical metrics based on which a specialised IT specialist understands whether everything is fine in the work of a certain AI/ML model, whether it has been relearned and whether there is a need to reconfigure the model as quickly as possible. For example, the war in Ukraine changed customers' behaviour, and the migration processes significantly increased. The bank promptly reconfigured the AI/ML models in accordance with new challenges and business tasks. The Central Bank also frequently changed currency legislation, the list of sanctioned persons changed every week, etc. The bank was forced to reconfigure its AI/ML models following the changes rapidly. It is important to note that representatives of the banks particularly emphasised the importance of making changes by the internal IT employees of the bank. It is connected not only with security but also with the need to make operational changes quite often.

The respondent of a large bank with a high level of digitalisation of operations noted that the bank operates more than 500 different systems (core banking systems, CRM systems and others), the vast majority of which are internal development by the bank's IT specialists. They make 10–30 releases of separate systems daily in the bank. As for the field of financial monitoring, releases with new rules are issued regularly, once every two weeks or even more frequently. Changes are made either directly to the system using ML models or directly to the AI model. In fact, the AI model cannot ensure that all problematic issues are fulfilled. The model should be correctly integrated into the business process. For transaction monitoring AI models, model implementation results should be properly used in the CRM system, in customer service processes, etc. Banks often release systems and make general changes to databases and models. Not all AI systems in the bank are integrated with each other, but those systems that require integration have it. Sometimes, this integration occurs through APIs, sometimes through the exchange of data streams, but not all of these systems use AI approaches. Typically, AI models are used in “on top of data” systems and risk-related tasks.

Considerable attention during the development and use of AI/ML systems is paid to their security and protection (resilience of AI) against cyber-attacks. Banks in Ukraine are extremely serious about the protection of their systems since cyber-attacks are frequent. Banks have created cyber security departments that try to block third-party intrusion particularly the cyber threats coming from Russia.

There is a bunch of multiple layers of encryption and various things like IP whitelisting, key backed protection systems and more. Banks have a risk matrix to identify potential threats and vulnerabilities within the AI/ML systems.

Another issue for AI/ML models is the issue of data pollution. The data science team had to work quite hard to ensure that their data is at a level of confidence and that AI/ML model could then do something useful and reliable with it. Another problem with AI/ML models is that the outputs are a product of the inputs. If the data itself is incomplete, inconsistent, or has holes, then the AI/ML model is going to generate a whole bunch of incorrect answers (false positives). In terms of the specific mechanisms of what is done with data, much work has gone into ensuring that the data you input into any AI model is consistent, accurate, and not filled with holes or anything missing.

Barriers to adoption of AI/ML systems by banks

Most respondents saw no reason why banks should not implement AI/ML systems. The advantages outweigh the disadvantages. The main question concerns what added value the implementation of AI/ML systems can provide. It depends on the bank's business model.

The decision to implement AI/ML systems is taken by each bank individually based solely on its spheres of activity and the diversity of the product line. Accordingly, the following questions should be answered:

- In which areas can the bank apply AI/ML models?
- Does the bank have an internal IT team capable of developing or maintaining AI systems?
- How strict are the requirements of the regulatory authorities?
- What fundamental data governance and quality processes are lacking in the bank?

Suppose the bank already has a certain foundation and has gradually digitised its products. In that case, the decision to use AI/ML models will prevail over a conservative approach, and the added value will be greater than the investment amount.

Significant regulatory scrutiny and huge potential fines deter banks from using certain advanced AI models without the relevant safeguards *inter alia*, transparency, traceability and explainability of AI/ML systems. One of the potential barriers to the adoption of complex AI/ML models is the lack of understanding by the end users of how the machine or the technology arrives at its outcomes. The bank is responsible for its clients' funds, so a conservative approach is usually adopted. This approach is typical for small banks that do not have the opportunity to develop their own AI/ML systems but order them from a third-party developer. The cost of such AI systems is significant, and changes to these systems also cost quite a lot of money.

Banks are cautious about purchasing AI/ML models from third-party developers not only because of the high cost. The risks of inaccuracy in the operation of the model in the bank will increase significantly, despite its effective configuration by the development company. For banks, the AI system is a kind of "black box" if purchased from a third-party organisation. Not every bank can afford the development of its own high-quality AI systems.

The banks use certain AI programs, such as card software products, mobile banking, and face and voice recognition. Third-party developers generally maintain these. However, programs related to financial monitoring and risk analysis of the bank's activities should preferably be monitored and maintained by their IT employees. It is quite a challenging task for small banks. That is why, considering all the pros and cons, banks use complicated AI systems cautiously, especially in the field of monitoring transactions. The respondent from Bank 2 mentioned that the bank has 1200 internal IT team personnel and mostly all AI products are developed in-house. That is partly the answer to why this bank uses AI/ML systems broadly, including transaction monitoring.

A specialised bank with a small number of clients adopted AI systems that would mainly serve their corporate clients and ensure cost efficiency. It is quite enough for such a bank to robotise certain processes to minimise employees' routine work, use rule-based and simple programs, and have expert rules for making decisions.

However, suppose it is a multi-branch bank that carries out various types of operations and hundreds of different credit and deposit products. In that case, even a small bank (about 1 million customers) must implement machine learning models, approaches in the field of AI, and increase the level of digitalisation of its products at the expense of AI. Such banks should not be afraid of implementing new AI/ML technologies.

In the EU Member States, compliance with AI/ML standards is becoming stricter; besides, the cost of implementing AI systems is substantial. In addition to significant investments, banks need to recruit a team of professional IT employees, as it is quite problematic to outsource a data team of employees. It is also necessary to strictly comply with the requirements of various supervisory authorities. Therefore, small banks often realise that the investment made in AI/ML systems will be greater than the potential added value they will bring to the bank.

Overarching themes

Interviewees indicated that any bank that wants to develop and respond to market competition should use modern AI technologies. The transition to new AI technologies requires a change in the bank's business model, which can be costly. Not every bank can afford it. Therefore, the problem primarily concerns financial capacity. It is a particularly complex challenge for small banks.

Another problematic issue emanates from a human factor. The desire and understanding of the need by the bank's top management is required. It applies to the bank's owners, management and employees. Not everyone is ready to change their approach to the bank's activities quickly and how its services are delivered.

Many banks are attracted to the idea or the potential of AI/ML systems can bring. The biggest concern for people not wanting to adopt AI/ML models centres around accountability, transparency and explainability issues. They need to be sure that the constructed AI technology is robust and

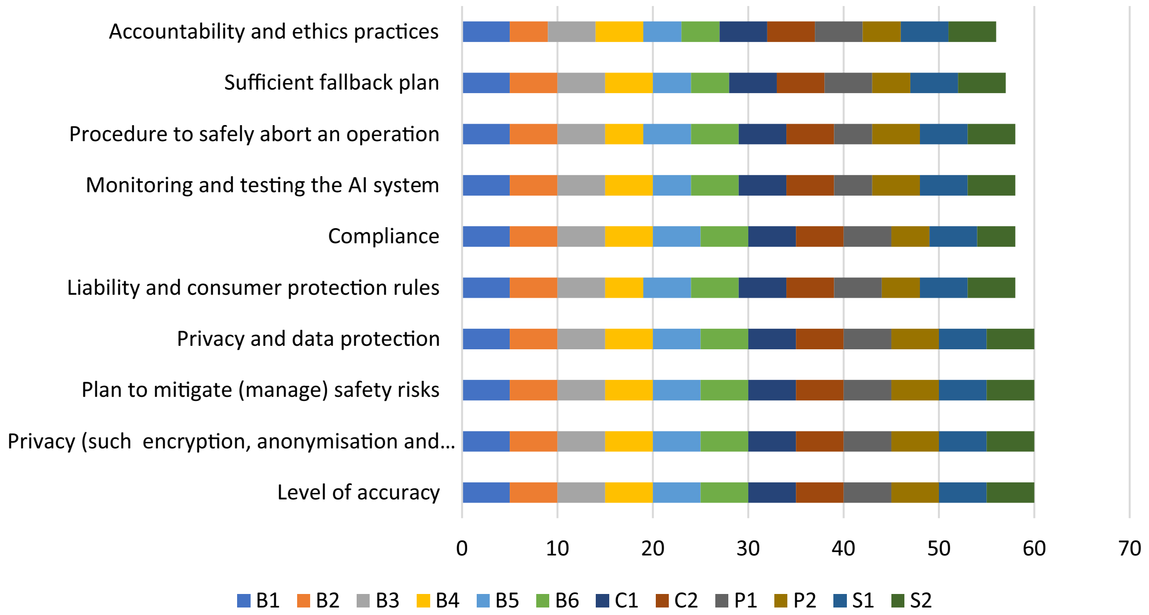

Fig. 2 TOP-10 priorities for AI/ML systems in transaction monitoring and AML Source: Authors' own compilation

transparent enough to show the workings that should be achieved.

The approach to implementing complex AI systems differs depending on the field of use. Banks in customer service, customer support, and marketing services (front-office activities) are easily switching to complex AI systems. They often use ready-made software solutions from third-party developers. The main consideration in this context is the cost-effectiveness.

Most banks have a different approach to areas of activity related to risk and compliance with the requirements of regulatory bodies. The areas of bank activity related to risk should be closely monitored by banks, and banks are conservative in the implementation of advanced AI systems.

Banks are also cautious in implementing sophisticated AI/ML systems in financial monitoring and money laundering operations. The supervisory bodies severely punish the bank for law violations, especially in AML/CFT. Therefore, banks prefer using simple AI and ML systems to monitor funds; specific scripts are used to track operations with signs of dubiousness. However, at the next stage, a person decides regarding each questionable operation or suspicious transaction. Banks prefer ultimate human control (human-in-the-loop) in this respect.

Another reason for not using complex AI models is that fraudsters can find vulnerabilities in complex AI systems, particularly if a third-party organisation develops the AI system and is not an internal product of the bank (in-house developed systems). That is one of the main reasons why banks try to develop and maintain such AI/ML systems using their own IT staff as much as possible.

At the same time, banks understand that processing a large data flow is difficult without modern AI/ML systems. Therefore, it is definitely necessary to have a high level of trust in such systems and use them accordingly. Such systems need to be improved constantly. If there are problematic points, then it is necessary to improve the algorithm quickly. It is impossible to predict all system vulnerabilities. At the same time, it is important for the bank to promptly correct the error, improve the algorithm, and thus solve the problem. There are many procedures and possibilities in every bank. The majority of these procedures are prescribed. If an unforeseen situation arises, banking AI programs always have the option of rolling back the program's action and rewriting the decision.

Such a vision of the bank's management of the risks of using complex AI/ML in the field of monitoring transactions and AML/CFT related operations is holding back progress in the application of complex AI/ML systems. Currently, banks prefer in-house AI systems, errors in which are easy to understand and can be quickly corrected by the bank's own IT employees.

Respondents consider the following features as a top priority for AI systems: level of accuracy, privacy and data protection, plan to mitigate (manage) safety risks, privacy (such as encryption, anonymisation and aggregation) (Fig. 2).

Respondents attach minor importance to: self-learning or autonomous AI systems, environmental impact, and internal user acceptance of AI/ML models (Fig. 3).

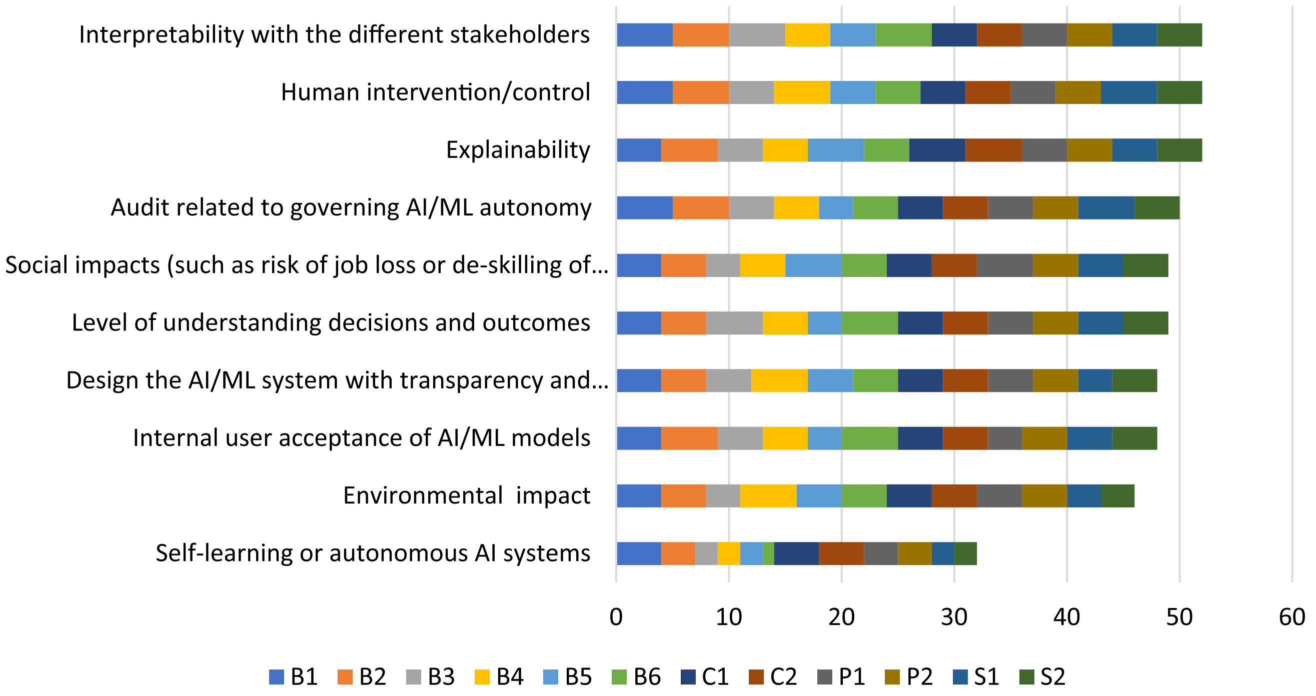

Fig. 3. 10 least important considerations for AI/ML systems in transaction monitoring and AML Source: Authors' own compilation

Case studies: lessons from misuse of AI tools

The cases selected demonstrate a number of cardinal issues that emerged in the interview discussions. Firstly, even some of the biggest banks in the world find full compliance with data management and monitoring suspicious transactions a challenge. Secondly, these cases reveal the serious consequences of non-compliance. Thirdly, analysis of these cases enables us to offer several AI-driven solutions that could minimise the risks involved. It should be noted that there are currently no concluded court cases pertaining to the proposed EU AI Act (as this law is not in force yet). However, past cases can offer important lessons for banks.

NatWest Bank—a unique case of corporate criminal liability

National Westminster Bank Plc (NatWest) was, in December 2021, fined £264.8 million for having breached the Money Laundering Regulations 2007 from 2012 to 2016 [59]. The infractions of AML regulations by NatWest were largely inadequate because due diligence mechanisms prescribed by the UK's AML regulation were not complied with. The case was heard at Southwark Crown Court on charges against NatWest for three offences pursuant to Regulation 45(1) of the Money Laundering Regulations 2007 (MLR 2007). The three offences were based on operational weaknesses of the bank vis-à-vis the bank's failure to adequately monitor the bank accounts of a customer incorporated in the UK. These were in breach of Regulations 8(1), 8(3), and 14(1) MLR 2007. On 7 October 2021, NatWest admitted [60] that it, indeed, committed these offences. Due to early guilty plea made by NatWest, the court discounted the originally intended fine by 33%.

The FCA decided to conclude the case without pursuing any bank officials. It appears that there was no further need for legal action against individuals. The problem facing NatWest was more in the nature of criminal corporate liability than individual liability. It is possible that investigators and prosecutors were constrained by lack of facts with evidential value to pursue natural persons in the bank or even outside the bank. With robust AML AI architecture in place, it could have been possible to crawl and interconnect data of evidential value.[7] It is, therefore, interesting that

[7] Data crawling (web crawling or web scraping) is a process in which automated software, called crawlers or spiders, systematically browse and extract information from various websites, databases or other online sources. These crawlers navigate through web pages, follow links, and retrieve data according to predefined rules or patterns. Crawling and interconnecting data of evidential value suggests a potential opportunity to gather and link together data that holds evidential significance. Collecting and integrating data with evidential value would have been feasible by employing data crawling techniques, implying the potential for a more comprehensive and interconnected understanding of the subject matter. See Khder, M. (2021) Web Scraping or Web Crawling: State of Art, Techniques, Approaches and Application. *International Journal of Advances in*

NatWest has already planned to invest more than £1 billion in order 'to further strengthen financial crime controls over the next five years' [59]. This investment includes pursuing 'new technologies and capabilities to enhance further CDD, Transaction Monitoring' and so on.

The FCA had, on 16 March 2021, begun criminal proceedings against NatWest pursuant to offences under Regulation 45(1) of the MLR 2007 for non-compliance with regulation 8(1) of the MLR 2007 from 7 November 2013 to 23 June 2016 as well as Regulations 8(3) and 14(1) of the MLR 2007 from 8 November 2012 to 23 June 2016 with respect to the bank accounts of a customer incorporated in the UK. The import of these regulations is to the effect that banks are required 'to determine and conduct risk sensitive ongoing monitoring of its customers for the purposes of preventing money laundering' [59].

NatWest, however, confirmed that some of the automated AI systems of the bank were weak and that the bank had some deficiencies in complying with AML procedures on monitoring and investigations. While this case is the first bank to face corporate criminal liability in the UK, it is imperative to underscore that the deficiencies in monitoring mechanisms by regulatory authorities such as the FCA also contributed to this non-compliance. If FCA had sophisticated AI systems, it should have been feasible to detect the weak systems by NatWest much earlier.

HSBC, Danske bank and standard chartered bank—the huge fines?

Hitherto the case of NatWest, the Danske Bank, HSBC and Standard Chartered Bank were respectively fined for about US$2 billion[8] [61], US$1.9 billion (£1.2bn)[9] and US$1.1 billion[10] [62] as a result of the failure of these banks to comply with relevant AML rules.

With respect to *HSBC*, the bank had been found guilty of not having established adequate AML control measures, which allowed about US$8 billion to be laundered for a period of seven years [63].

In the case of *Danske Bank*, the Estonian branch of the bank was accused of having allowed, due to weak AML controls, thousands of suspicious illicit transactions amounting to about EUR 200 billion[11] between 2007 and 2015 [64]. The illicit money flows (IMFs) were carried out from sources such as Latvia, Estonia, and Russia through the Estonian branch of Danske Bank [65]. Up to 15,000 non-resident customers were involved in this, many of whom being Russian. Additionally, 9.5 million payments were made while searches were conducted in about 12,000 documents and over 8 million emails [64, 66]. The risk assessment AI tool used by Danske Bank erroneously excluded high and medium risk customers thus ended up providing inaccurate and biased outputs.

The Standard Chartered Bank was also found guilty of AML due diligence negligence and fined for US$1.1 billion. This fine was the total fine for US and UK sanctions against the bank for its 'poor money-laundering controls' as well as its breach of sanctions against countries such as Iran. The FCA had conducted investigations into these higher-risk areas and found 'serious and sustained shortcomings' in Standard Chartered's AML controls with respect to 'CDD and ongoing monitoring' [67]. The bank had not been able 'to establish and maintain risk-sensitive policies and procedures', in contravention of the MLRs 2007, exposing the bank 'to the risk of … receiving and/or laundering the proceeds of crime' [67]. Many examples were found. One of the points of interest is the finding that the bank was 'not reviewing due diligence on a customer despite repeated red flags such as a blocked transaction from another bank indicating a link to a sanctioned entity' [67].

Conclusions

This study is built on the qualitative research design, interviewing senior managers of banks, IT companies and comparing their answers. The results are described from the perspective of the bank's managers. The findings show the importance of AI/ML systems in banks, the further willingness of banks to use such systems more deeply, and the main caveats regarding the problematic aspects of implementing AI/ML systems mainly relate to their cost and economic efficiency.

Our empirical study reveals not only some of the drivers for adopting AI tools in banking but also a number of impediments or factors for not doing so. These findings also reveal the level of understanding of the required ethical and legal standards pertaining to the use of AI/ML technologies in the banking sector.

The selected case studies demonstrate that even the most prominent banks are prone to non-compliance with AML/

Footnote 7 (continued)

Soft Computing and its Applications 13: 145-168, https://doi.org/10.15849/IJASCA.211128.11.

[8] This amount is estimated potential fine by USA authorities and actual fine of €1,820,000 by the Central bank of Ireland (Central Bank of Ireland, 2022).

[9] Settlement by authorities of USA.

[10] Settlement by UK and USA authorities.

[11] This value was estimated to be a staggering 10 times of the Gross Domestic Product of Estonia. See [64].

CFT standards, which come with serious consequences. Our critique of these cases offers a number of solutions for risk mitigation and better compliance protocols, which could be addressed by fit-for-purpose AI-driven tools.

Funding Research for this paper received funding from the Horizon 2020 Programme [TRACE-AI in countering financial crime and tracing illicit money flows—Grant Agreement No: 101022004—https://trace-illicit-money-flows.eu] and the ECB Legal Research Programme 2022.

Declarations

Conflict of interest On behalf of all authors, the corresponding author states that there is no conflict of interest.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0/.

References

1. FATF. 2021. Opportunities and challenges of new technologies for AML/CFT. FATF, July, https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf, Accessed 02 Nov 2022.
2. OECD. 2021. Artificial intelligence, machine learning and big data in finance opportunities, challenges and implications for policy makers'. OECD, https://www.oecd.org/finance/financial-markets/Artificial-intelligence-machine-learning-big-data-in-finance.pdf, Accessed 20 Apr 2023.
3. MHC. 2022. Resolving regulatory challenges. Mansion House Consulting, 19 July, https://www.mansion-house.co.uk/articles/resolving-regulatory-challenges/, Accessed 21 Sept 2022.
4. An, J., and R. Rau. 2021. Finance, technology and disruption. *The European Journal of Finance* 27 (4–5): 334–345. https://doi.org/10.1080/1351847X.2019.1703024.
5. Dennehy, D. 2020. Ireland post-pandemic: utilising AI to kick-start economic recovery. *Cutter Business Technology Journal* 33 (11): 22–27.
6. Collins, C., D. Dennehy, K. Conboy, and P. Mikalef. 2021. Artificial intelligence in information systems research: a systematic literature review and research agenda. *International Journal of Information Management* 60 (102383): 1–17.
7. McCarthy, J. 2007. What is artificial intelligence?, Stanford University, 12 November, https://jmc.stanford.edu/articles/whatisai/whatisai.pdf, Accessed 11 May 2023.
8. Copeland, B.J. 2022. Artificial intelligence. Definition, examples, and applications. *Encyclopedia Britannica*, https://www.britannica.com/technology/artificial-intelligence, Accessed 11 May 2023.
9. von Rueden, L., S. Mayer, K. Beckh, B. Georgiev, S. Giesselbach, R. Heese, et al. 2023. Informed machine learning—a taxonomy and survey of integrating prior knowledge into learning systems. *IEEE Transactions on Knowledge and Data Engineering* 35 (1): 614–633. https://doi.org/10.1109/TKDE.2021.3079836.
10. Janiesch, C., P. Zschech, and K. Heinrich. 2021. Machine learning and deep learning. *Electron Markets* 31: 685–695. https://doi.org/10.1007/s12525-021-00475-2.
11. Abdar, M., F. Pourpanah, S. Hussain, D. Rezazadegan, L. Liu, M. Ghavamzadeh, et al. 2021. A review of uncertainty quantification in deep learning: techniques, applications and challenges. *Information Fusion* 76: 243–297. https://doi.org/10.1016/j.inffus.2021.05.008.
12. Linardatos, P., V. Papastefanopoulos, and S. Kotsiantis. 2020. Explainable AI: a review of machine learning interpretability methods. *Entropy* 23 (1): 1–45. https://doi.org/10.3390/e23010018.
13. Joseph, J., and U. Turksen. 2022. Harnessing AI for due diligence in CBI programmes: legal and ethical challenges. *Journal of Ethics and Legal Technologies* 4 (2): 9–12.
14. Davenport, T. and Ronanki, R. 2018. Artificial intelligence for the real world. *Harvard Business Review*, January-February: 108–116, http://blockqai.com/wp-content/uploads/2021/01/analytics-hbr-ai-for-the-real-world.pdf, Accessed 8 May 2023.
15. Fintech Futures. 2022. AI in FinTech global market report 2022: Key Players Microsoft, Google, IBM & Others Driving 27.6% Annual Growth. *Globe Newswire*, 30 August. https://www.fintechfutures.com/techwire/ai-in-fintech-global-market-report-2022-key-players-microsoft-google-ibm-others-driving-27-6-annual-growth/, Accessed 02 Nov 2022.
16. Gov.uk 2022. The benefits and harms of algorithms: a shared perspective from the four digital regulators. *Research and analysis, Discussion paper*, 23 September, https://www.gov.uk/government/publications/findings-from-the-drcf-algorithmic-processing-workstream-spring-2022/the-benefits-and-harms-of-algorithms-a-shared-perspective-from-the-four-digital-regulators, Accessed 03 Nov 2022.
17. Tsamados, A., N. Aggarwal, J. Cowls, J. Morley, H. Roberts, M. Taddeo, et al. 2022. The ethics of algorithms: key problems and solutions. *AI & Society* 37: 215–230.
18. Wang, R., J. Liu, and H. Luo. 2021. Fintech development and bank risk taking in China. *The European Journal of Finance* 27 (4–5): 397–418.
19. Adamyk, O., Chereshnyuk, O., Adamyk, B. and Rylieiev, S. 2023. Trustworthy AI: a fuzzy-multiple method for evaluating ethical principles in AI regulations. *13th IEEE International Conference on Advanced Computer Information Technologies*, doi: https://doi.org/10.1109/ACIT58437.2023.10275505.
20. Van der Burgt, J. 2019. General principles for the use of Artificial Intelligence in the financial sector. De Nederlandsche Bank, https://www.dnb.nl/media/voffsric/general-principles-for-the-use-of-artificial-intelligence-in-the-financial-sector.pdf, Accessed 20 Sept 2022.
21. Malviya, R. 2022. Leveraging AI in quality assurance. *Infosys*, https://www.infosys.com/insights/ai-automation/quality-assurance.html, Accessed 07 Nov 2022.
22. Gartner. 2021. Industrywide funding for AI expected to increase through 2022. Gartner, 29 September, https://www.gartner.com/en/newsroom/press-releases/2021-09-29-gartner-finds-33-percent-of-technology-providers-plan-to-invest-1-million-or-more-in-ai-within-two-year, Accessed 04 Nov 2022.
23. Glikson, E., and A. Woolley. 2020. Human trust in artificial intelligence: review of empirical research. *Academy of Management Annals* 14 (2): 2022. https://doi.org/10.5465/annals.2018.0057,accessed02November.
24. Owczarek, D. 2022. AI in banking. Applications and benefits of artificial intelligence in financial services. *Nexocode*, 29 March, https://nexocode.com/blog/posts/ai-in-banking.appli

cations-and-benefits-of-artificial-intelligence-in-financial-services/, Accessed 12 Nov 2022.

25. Digalaki, E. 2022. The impact of artificial intelligence in the banking sector & how AI is being used in 2022. *Insider*, 2 February, https://www.businessinsider.com/ai-in-banking-report?r=US&IR=T, Accessed 11 Nov 2022.
26. Fintegral. 2022. AI and machine learning for credit rating models–Part I. A brief overview of the regulatory landscape. Fintegral, 30 March, https://www.fintegral.com/storage/app/media/uploaded-files/20220330ai-and-machine-learning-for-credit-rating-models-part-ifinal.pdf, Accessed 15 Sept 2022.
27. Guerra, P., and M. Castelli. 2021. Machine learning applied to banking supervision a literature review. *Risks* 9 (136): 1–24. https://doi.org/10.3390/risks9070136.
28. Central Bank of Ireland. 2021. Anti-money laundering and countering the financing of terrorism guidelines for the financial sector. Central Bank of Ireland, https://www.centralbank.ie/docs/default-source/regulation/amld-/guidance/anti-money-laundering-and-countering-the-financing-of-terrorism-guidelines-for-the-financial-sector.pdf?sfvrsn=64d4bc1d_11, Accessed 15 Sept 2022.
29. Eurojust. 2022. Eurojust report on money laundering. Eurojust, October, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust-report-money-laundering-2022.pdf, Accessed 12 Mar 2023.
30. Benson, V., U. Turksen, and B. Adamyk. 2023. Dark side of decentralised finance: a call for enhanced AML regulation based on use cases of illicit activities. *Journal of Financial Regulation and Compliance*. https://doi.org/10.1108/JFRC-04-2023-0065.
31. Kyckr. 2021. White paper: AML fines report 2021. Kyckr, 7 November, https://www.kyckr.com/resourcegated/aml-fines-report-2021, Accessed 16 Sept 2022.
32. Felzmann, H., E. Fosch-Villaronga, C. Lutz, and A. Tamò-Larrieux. 2020. Towards transparency by design for artificial intelligence. *Science and Engineering Ethics* 26 (6): 3333–3361.
33. Surkov, A., Srinivas, V. and Gregorie, J. 2022. Unleashing the power of machine learning models in banking through explainable artificial intelligence (XAI). *Deloitte Insights*, 17 May, https://www2.deloitte.com/uk/en/insights/industry/financial-services/explainable-ai-in-banking.html, Accessed 02 Nov 2022.
34. Reynolds, B., Donegan, T., Collins, S. and Barrowman, C. 2021. The future of financial regulation in the UK. *Shearman&Sterling*, 10 May, https://www.shearman.com/Perspectives/2021/05/The-Future-of-Financial-Regulation-in-the-UK, Accessed 04 Nov 2022.
35. Penn, B., Dumitru R. and Hadfield, M. 2022. Banking regulation in the United Kingdom: overview. *Allen & Overy LLP*, 1 April, ,https://uk.practicallaw.thomsonreuters.com/w-008-0211?transitionType=Default&contextData=(sc.Default)&firstPage=true, Accessed 05 Nov 2022.
36. Cheatham, B., Javanmardian, K. and Samandari, S. 2019. Confronting the risks of artificial intelligence. *McKinsey Quarterly*, 26 April, https://www.mckinsey.com/capabilities/quantumblack/our-insights/confronting-the-risks-of-artificial-intelligence, Accessed 08 Nov 2022.
37. Holden, A. 2021. 7 Biggest challenges of KYC monitoring. *FinExtra*, 11 February, https://www.finextra.com/blogposting/19866/7-biggest-challenges-of-kyc-monitoring, Accessed 07 Nov 2022.
38. Coelho, R., Fishman, J. and Ocampo, D.G. 2021. Supervising cryptoassets for anti-money laundering. *BIS, FSI Insights on policy implementation*, no. 31, April, https://www.bis.org/fsi/publ/insights31.pdf, Accessed 07 Nov 2022.
39. Bank of England. 2019. Machine learning in UK financial services. Bank of England, October, https://www.bankofengland.co.uk/-/media/boe/files/report/2019/machine-learning-in-uk-financial-services.pdf?la=en&hash=F8CA6EE7A5A9E0CB182F5D568E033F0EB2D21246, Accessed 17 Sept 2022.
40. Buchanan, B., and D. Wright. 2021. The impact of machine learning on UK financial services. *Oxford Review of Economic Policy* 37 (3): 537–563.
41. Ayadurai, C. and Joneidy, S. 2021. Artificial intelligence and bank soundness: between the devil and the deep blue sea—Part 2. In: *Operations Management—Emerging Trend in the Digital Era. IntechOpen*, pp. 1–14, doi: https://doi.org/10.5772/intechopen.95806.
42. Bank of England. 2022. Artificial intelligence and machine learning. Discussion paper 5/22. 11 October. https://www.bankofengland.co.uk/prudential-regulation/publication/2022/october/artificial-intelligence, Accessed 1 Nov 2022.
43. Danielsson, J., Macrae, R. and Uthemann, A. 2020. Artificial intelligence as a central banker. *CEPR*, 6 March, https://cepr.org/voxeu/columns/artificial-intelligence-central-banker, Accessed 18 Sept 2022.
44. Boukherouaa, E.B., G. Shabligh, K. AlAjmi, J. Deodoro, A. Farias, E.S. Iskender, et al. 2022. Powering the digital economy: opportunities and risks of artificial intelligence in finance. *IMF, Departmental Papers* 2021 (024): 1–31. https://doi.org/10.5089/9781589063952.087,accessed28November.
45. Danielsson, J., R. Macrae, and A. Uthemann. 2022. Artificial intelligence and systemic risk. *Journal of Banking & Finance*. https://doi.org/10.1016/j.jbankfin.2021.106290.
46. European Commission. 2021. Press corner. European Commission, 21 April, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683, Accessed 20 Sept 2022.
47. Ebers, M. 2022. Standardising AI—The Case of the European Commission's proposal for an artificial intelligence Act. In: Larry A. DiMatteo, Cristina Poncib and Michel Cannarsa (eds.). The Cambridge Handbook of Artificial Intelligence: Global Perspectives on Law and Ethics (Cambridge University Press 2022), p. 43.
48. Edwards, L. 2022. The EU AI Act: a summary of its significance and scope. Ada Lovelace Institute, April, https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf, Accessed 11 May 2023.
49. Veale, M., and F. ZuiderveenBorgesius. 2021. Demystifying the draft EU artificial intelligence act—analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International* 22 (4): 97–112.
50. NBU. 2020. Fintech development strategy in Ukraine until 2025. *The National Bank of Ukraine*, July (in Ukrainian), https://bank.gov.ua/admin_uploads/article/Strategy_finteh2025.pdf?v=4, Accessed 8 Mar 2023.
51. FSB. 2020. The use of supervisory and regulatory technology by authorities and regulated institutions market developments and financial stability implications. *Financial Stability Board*, October, https://www.fsb.org/wp-content/uploads/P091020.pdf, Accessed 12 Nov 2022.
52. Eichengreen, B. 2023. Financial regulation in the age of the platform economy. *Journal of Banking Regulation* 24: 40–50. https://doi.org/10.1057/s41261-021-00187-9.
53. UK Finance, EY. 2020. Trust, context and regulation: achieving more explainable AI in financial services. UK Finance, Ernst and Young, October, https://www.ukfinance.org.uk/system/files/Trust%2C%20Context%20and%20Regulation%20-%20Achieving%20more%20explainable%20AI%20in%20financial%20services.pdf, Accessed 11 Sept 2022.
54. McWaters, R., Blake, M. and Galaski, R. 2019. Navigating Uncharted waters: a roadmap to responsible innovation with AI in financial services. Part of the future of financial services series. *World Economic Forum*, 23 October, https://www.weforum.org/reports/navigating-uncharted-waters-a-roadmap-to-respo

nsible-innovation-with-ai-in-financial-services/, Accessed 14 Sept 2022.

55. BarredoArrieta, A., N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, et al. 2020. Explainable artificial intelligence (XAI): concepts, taxonomies, opportunities and challenges toward responsible AI. *Information Fusion* 58 (1): 82–115.
56. Van den Berg, M. and Kuiper, O. 2020. A conceptual framework for explainable AI (XAI). XAI in the financial sector. *Hogeschool Utrecht, Lectoraat Artificial Intelligence Version 1.1*., https://www.internationalhu.com/research/projects/explainable-ai-in-the-financial-sector, Accessed 15 Sept 2022.
57. Kuiper, O., van der Burgt, J., Leijnen, S. and van den Berg, M. 2021. Exploring explainable AI in the financial sector: perspectives of banks and supervisory authorities. *ResearchGate*, November, https://www.researchgate.net/publication/355809049_Exploring_Explainable_AI_in_the_Financial_Sector_Perspectives_of_Banks_and_Supervisory_Authorities, Accessed 15 Sept 2022.
58. Miller, T. 2019. Explanation in artificial intelligence: Insights from the social sciences. *Artificial Intelligence* 267: 1–38. https://doi.org/10.1016/j.artint.2018.07.007.
59. NatWest. 2021a. National Westminster Bank Plc fined £264.8m for breaches of Regulation. 13 December, https://www.natwestgroup.com/news/2021/12/nwb-plc-fined-for-breaches-of-regulations.html, Accessed 8 Nov 2022.
60. NatWest. 2021b. National Westminster Bank Plc pleads guilty to breaches of Regulations. 7 October, https://www.natwestgroup.com/news/2021/10/national-westminster-bank-plc-pleads-guilty-to-breaches-of-regulations.html, Accessed 8 Nov 2022.
61. Milne, R. 2022. Danske Bank braced for money-laundering fines of $2bn. *Financial Times*, 27 October, https://www.ft.com/content/8535bf21-fb42-4177-a7a6-d1f053d398e9, Accessed 8 Nov 2022.
62. Credas. 2023. The biggest banking AML Fines. *Credas*, 23 February, https://credas.co.uk/resources/the-biggest-banking-aml-fines/, Accessed 8 May 2023.
63. BBC News. 2012. HSBC to pay $1.9bn in US money laundering penalties. *BBC News*, 11 December, https://www.bbc.co.uk/news/business-20673466, Accessed 8 Nov 2022.
64. Coppola, F. 2018. The tiny bank at the heart of Europe's Largest money laundering scandal. *Forbes*, 26 September, https://www.forbes.com/sites/francescoppola/2018/09/26/the-tiny-bank-at-the-heart-of-europes-largest-money-laundering-scandal/, Accessed 8 Nov 2022.
65. Danske Bank. 2022. The investigations relating to Danske Bank's Estonian branch. Danske Bank, https://danskebank.com/about-us/corporate-governance/investigations-on-money-laundering Accessed 8 Nov 2022.
66. Danske Bank. 2018. Findings of the investigations relating to Danske Bank's branch in Estonia. *Press Releases*, 19 September, https://danskebank.com/news-and-insights/news-archive/press-releases/2018/pr19092018, Accessed 8 Nov 2022.
67. FCA. 2019. FCA fines Standard Chartered Bank £102.2 million for poor AML controls. FCA, 9 April, https://www.fca.org.uk/news/press-releases/fca-fines-standard-chartered-bank-102-2-million-poor-aml-controls, Accessed 8 Nov 2022.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Umut Turksen is Professor in Law at the Centre Financial and Corporate Integrity of Coventry University. Umut is a business-facing legal academic, and he is interested in the practical application of the law in innovation, societal security and development. He has provided consultancy and training to prestigious international businesses and government projects. He led the EU funded project "PROTAX," which focused on the countering tax crimes in Europe and he is currently coordinating another EU funded project, TRACE, (https://trace-illicit-money-flows.eu) which aims to create technology based solutions (including AI) for tracking illicit money flows. In addition to his expertise in financial crime, societal security, risk and compliance, Umut has published extensively on energy law and security, international trade law and development, and arbitration.

Vladlena Benson is Professor of Cyber Security Management, directs the Cyber Security Innovation Centre at Aston University, UK. Her research focuses primarily on secure FinTech exploitation, cyber security risk management and privacy enhancing technologies, which is published by world-leading journals. Alongside her academic role, Vladlena is working with multiple organisations and governments, moulding future national policy within Cyber Security, Standards and Partnerships. This includes Membership of the UK Cyber Security Council (UK CSC) and Information Systems Audit and Control Association (ISACA), serving on the European Union Agency for Cybersecurity (ENISA) task force defining the criteria for European Cybersecurity Framework at the EU level.

Bogdan Adamyk is Research Fellow at the Cyber Security Innovation Centre, Aston University, UK**.** He is an experienced researcher, having published in top-rated academic journals and edited volumes, and his publications enjoy a high level of popularity as he specialises in banking regulation and cryptocurrency. Bogdan works on the Horizon-funded project TRACE-AI in countering financial crime and tracing illicit money flows at Aston Business School. His current research interests lie in the area of AI regulation, cryptocurrencies, and blockchain applications in finance.