World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

Harnessing artificial intelligence for combating money laundering and fraud in the U.S. financial industry: A comprehensive analysis

Omogbolahan Alli [1,*], Okechukwu Eze Chigbu [2], Chinedu Mbabie [3], Ajibola Olapade [3], Vivian Kiniga [4] and Karl Kiam [5]

[1] *Department of Electrical Engineering, University of Ibadan, Ibadan Nigeria.*
[2] *College of Business, University of Louisville, Kentucky USA.*
[3] *Department of Computer Science, University of Lagos, Akoka, Lagos Nigeria.*
[4] *Department of Information Science, Cornell University, New York USA.*
[5] *Data Science and Analytics Institute, University of Oklahoma, Norman USA.*

World Journal of Advanced Research and Reviews, 2023, 17(02), 940-953

Received on 22 November 2022; revised on 25 February 2023; accepted on 27 February 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.17.2.0227

Abstract

The increasing sophistication of financial crimes, particularly money laundering and fraud, has necessitated the adoption of advanced technological solutions in the U.S. financial industry. Artificial Intelligence (AI) has emerged as a critical tool in combating these illicit activities by enhancing detection, prevention, and compliance mechanisms. This research explores and analyses the role of AI in countering money laundering and fraud, assessing its effectiveness, challenges, and regulatory implications. A qualitative research methodology was employed, utilizing secondary data sources, including reports from regulatory bodies, financial institutions, and academic literature. This approach provided a comprehensive analysis of AI-driven anti-money laundering (AML) solutions, emphasizing their impact on transaction monitoring, anomaly detection, and risk assessment. The research also examined key challenges, such as data privacy concerns, algorithmic biases, and regulatory compliance, which hinder AI's full potential in financial crime prevention. Findings reveal that while AI significantly improves fraud detection capabilities, its implementation remains constrained by regulatory gaps and concerns regarding transparency and fairness. Public-private partnerships, secure data-sharing frameworks, and robust AI governance structures are essential to ensuring ethical and effective AI deployment in the financial sector. The research concludes that AI holds immense promise in strengthening AML and fraud prevention strategies but requires continuous innovation and regulatory alignment to maximize its effectiveness.

Keywords: Artificial Intelligence (Ai); Money Laundering; Machine Learning; Algorithm; Fraud; Anti-Money Laundering (Aml)

1. Introduction

Money laundering and financial fraud have long posed significant threats to the integrity of the U.S. financial industry [1]. These illicit activities not only undermine economic stability but also facilitate various forms of organized crime. Historically, the U.S. has implemented stringent regulations, such as the Bank Secrecy Act and the USA PATRIOT Act, to combat these threats [2]. Despite these efforts, financial institutions continue to face challenges in effectively detecting and preventing sophisticated money laundering schemes. For instance, recent enforcement actions have resulted in substantial penalties for banks failing to comply with anti-money laundering (AML) regulations, underscoring the ongoing vulnerabilities within the system [2].

* Corresponding author: Omogbolahan Alli.

In recent years, artificial intelligence (AI) has emerged as a transformative force in enhancing financial crime detection and prevention. AI technologies, including machine learning algorithms and natural language processing, enable the analysis of vast datasets to identify patterns indicative of fraudulent activities [3]. Financial institutions are increasingly integrating AI into their AML frameworks to improve the accuracy and efficiency of monitoring systems [4]. This shift towards AI-driven solutions represents a significant advancement in the fight against financial crime [5].

Traditional AML and fraud detection mechanisms have often relied on rule-based systems and manual reviews [6]. While these methods have been foundational, they are limited by their rigidity and susceptibility to high false-positive rates [5, 6]. The static nature of rule-based systems makes them less adaptable to evolving money laundering techniques, necessitating more dynamic approaches [7].

The primary objective of this research is to examine how AI can enhance AML and fraud prevention efforts within the U.S. financial industry. By evaluating the integration of AI technologies into existing compliance frameworks, the research aims to identify improvements in detection accuracy, operational efficiency, and regulatory compliance.

1.1. The research will address the following questions:

- How can AI-driven technologies enhance the detection and prevention of money laundering and financial fraud in the U.S. financial industry?
- To what extent has AI been effective in reducing financial crime in the U.S., and what are the key barriers preventing its full potential in the financial industry?
- What are the comparative advantages of AI-driven systems over traditional AML methods in terms of adaptability and accuracy?
- What challenges do financial institutions face when integrating AI into their AML frameworks, and how can these be mitigated?

The study hypothesizes that AI integration significantly enhances the effectiveness of AML programs by reducing false positives and adapting to emerging money laundering techniques more efficiently than traditional methods.

This research holds substantial significance for various stakeholders. For financial institutions, adopting AI can lead to more robust AML strategies, reducing the risk of regulatory penalties and reputational damage. Regulatory bodies may benefit from insights into how AI can be leveraged to strengthen compliance requirements and oversight mechanisms. Policymakers could utilize the findings to craft legislation that supports technological innovation while ensuring the financial system's integrity. Ultimately, this study aims to contribute to a deeper understanding of AI's role in transforming AML efforts, promoting a more secure and resilient financial industry.

2. Conceptual and theoretical framework

In addressing the application of Artificial Intelligence (AI) to combat money laundering and fraud within the U.S. financial industry, it is essential to establish a comprehensive conceptual and theoretical framework. This involves defining key terms and exploring pertinent theories that elucidate the dynamics of financial crimes and the potential of AI in mitigating such illicit activities.

2.1. Definition of Key Terms

- Artificial Intelligence (AI): AI refers to the capability of machines, particularly computer systems, to mimic cognitive functions typically associated with human intelligence, such as learning, reasoning, and problem-solving [8]. In the financial sector, AI encompasses technologies that enable systems to analyze vast datasets, recognize patterns, and make decisions, thereby enhancing the detection and prevention of fraudulent activities [9].
- Machine Learning (ML): A subset of AI, machine learning involves algorithms that enable computers to learn from and make predictions or decisions based on data [10]. Unlike traditional programming, where explicit instructions are provided, ML models identify patterns within data, allowing systems to improve their performance over time without explicit reprogramming [11]. In anti-money laundering (AML) efforts, ML algorithms can detect unusual transaction patterns that may signify illicit activities.
- Money Laundering: This process involves concealing the origins of illegally obtained money, typically by means involving complex financial transactions, to make it appear legitimate [12]. The stages of money laundering include placement (introducing illicit funds into the financial system), layering (disguising the trail to obscure detection), and integration (merging the laundered money into the legitimate economy) [13].

- Fraud: Fraud encompasses wrongful or criminal deception intended to result in financial or personal gain. In the financial sector, this includes activities such as identity theft, credit card fraud, and securities fraud, where individuals or entities deceitfully misrepresent information for economic benefit [14].
- Financial Crime: A broader term that includes both money laundering and fraud, financial crime refers to any non-violent crime resulting in financial loss, typically involving deceit or breach of trust [15]. This category also covers offenses like bribery, corruption, and tax evasion, all of which undermine the integrity of financial systems.

2.2. Theoretical Framework

Integrating theoretical frameworks from criminology and organizational studies with advancements in artificial intelligence (AI) provides a comprehensive approach to combating money laundering and fraud in the U.S. financial industry. This synthesis focuses on four pivotal theories: Routine Activity Theory (RAT), Fraud Triangle Theory, Institutional Theory, and Machine Learning Theory. Each offers unique insights into the mechanisms of financial crimes and the potential of AI to mitigate these illicit activities.

2.2.1. Routine Activity Theory

Proposed by Lawrence E. Cohen and Marcus Felson in 1979, RAT posits that the occurrence of a crime is contingent upon the convergence of three elements: a motivated offender, a suitable target, and the absence of capable guardianship [16]. In the context of financial crimes, the "motivated offender" represents individuals or entities intent on engaging in money laundering or fraudulent activities [17]. The "suitable target" could be vulnerable financial systems or institutions, and the "absence of capable guardianship" signifies inadequate monitoring mechanisms [16, 17]. The digitalization of financial services has further expanded these opportunities. Online banking, mobile payments, and cryptocurrency transactions have introduced new platforms where traditional guardianship is limited.

AI enhances the "capable guardianship" component by introducing sophisticated surveillance systems capable of real-time transaction monitoring. Machine learning algorithms can analyze vast datasets to detect and flag unusual or anomalous transaction patterns indicative of fraudulent behaviour.

2.2.2. Fraud Triangle Theory

Developed by Donald Cressey in 1953, the Fraud Triangle Theory elucidates that fraud arises when three factors coalesce: perceived pressure (motivation), perceived opportunity, and rationalisation [18]. Perceived pressure refers to the individual's impetus to commit fraud, such as financial distress. Perceived opportunity denotes the circumstances that allow fraud to occur, often due to weak internal controls. Rationalisation involves the justifications individuals concoct to legitimize their dishonest actions [19].

AI can mitigate the "opportunity" aspect by fortifying internal controls within financial institutions. Advanced AI systems can automate the detection of irregularities in financial records, ensuring that discrepancies are promptly identified and addressed. For example, AI algorithms can scrutinize employee behaviours and transaction records to uncover potential collusion or unauthorized activities. By reducing opportunities for fraud through AI-enhanced oversight, institutions can disrupt the fraud triangle and prevent fraudulent incidents.

2.2.3. Institutional Theory

Articulated by W. Richard Scott in 1995, Institutional Theory examines how institutional environments influence organizational structures and behaviours [20]. It emphasizes that organizations are shaped by the norms, values, and regulations prevalent in their operating environment [21].

In the realm of financial crime prevention, AI can assist institutions in aligning with regulatory norms and societal expectations. AI-driven compliance tools can interpret and implement complex regulatory requirements, ensuring that financial institutions adhere to legal standards. AI can facilitate the standardization of compliance procedures across institutions, promoting consistency and transparency [22].

2.2.4. Machine Learning Theory

Machine Learning Theory underpins the development of algorithms that enable computers to learn from data and make informed decisions [10, 23]. In the context of financial crime detection, machine learning models can be trained to identify patterns associated with fraudulent activities. For example, supervised learning algorithms can utilize labelled

datasets of past fraudulent and legitimate transactions to predict the likelihood of new transactions being fraudulent. Unsupervised learning techniques, such as clustering, can detect novel fraud patterns without prior labelling [24].

Deep learning, a subset of machine learning, employs neural networks to analyze complex and high-dimensional data. In fraud detection, deep learning models can process intricate transactional data to uncover subtle correlations indicative of fraudulent behaviour [25]. The Machine Learning Theory, if leveraged, AI systems can continuously evolve and adapt to emerging fraud tactics, providing a dynamic defense mechanism against financial crimes.

2.2.5. Integration of the Theories

Combining these theoretical frameworks offers a holistic strategy for utilizing AI in the fight against money laundering and fraud. RAT and the Fraud Triangle Theory provide insights into the situational and psychological precursors of financial crimes, highlighting areas where AI can intervene to disrupt criminal activities. Institutional Theory underscores the importance of aligning AI applications with organizational norms and regulatory standards, ensuring that technological interventions are both effective and compliant. Machine Learning Theory offers the technical foundation for developing AI systems capable of detecting and preventing fraudulent activities through data-driven insights.

By integrating these theories, financial institutions can develop AI-driven systems that not only detect and prevent fraudulent activities but also align with organizational values and regulatory requirements. This comprehensive approach ensures that AI serves as a robust tool in safeguarding the integrity of the financial system.

3. Overview of money laundering and financial fraud in the United States of America

3.1. Historical Evolution and Key Case Studies.

Money laundering and financial fraud in the United States have evolved significantly over the past century, shaped by economic changes, regulatory developments, and high-profile criminal cases. The term "money laundering" is believed to have originated during the 1920s Prohibition era, when organized crime figures like Al Capone sought to disguise illicit alcohol profits by funnelling them through cash-intensive businesses such as laundromats [26]. This period highlighted the need for financial transparency, but the regulatory framework to combat such activities remained underdeveloped. By the 1970s, concerns over financial crime intensified, leading to the enactment of the Bank Secrecy Act (BSA) in 1970, which mandated financial institutions to maintain records and report transactions exceeding $10,000 [27]. This legislation marked the first major step in establishing financial oversight in the U.S., laying the foundation for future anti-money laundering (AML) regulations. The Watergate scandal further underscored the importance of financial transparency, as investigators traced illicit campaign funds through complex financial transactions, reinforcing the need for stricter regulations [28].

The 1980s saw a dramatic increase in drug trafficking, which fuelled a surge in money laundering activities. In response, the U.S. government introduced the Money Laundering Control Act of 1986, which explicitly criminalized money laundering and expanded enforcement mechanisms [29]. This law not only targeted those who laundered illicit funds but also introduced civil and criminal forfeiture provisions for violations of financial regulations. The focus on money laundering enforcement continued into the 1990s, with increasing scrutiny of financial institutions' compliance with AML regulations. However, despite regulatory efforts, financial fraud and corporate misconduct remained prevalent, as evidenced by the Enron scandal in 2001. Enron, once a highly regarded energy company, collapsed due to widespread accounting fraud, where executives used complex financial instruments to conceal debt and inflate profits [30]. The fallout from Enron's collapse led to the passage of the Sarbanes-Oxley Act of 2002, which imposed stricter corporate governance and financial reporting requirements to prevent similar fraudulent schemes [30].

In 2008, the exposure of Bernie Madoff's Ponzi scheme further demonstrated the sophistication of financial fraud in the modern era. Madoff defrauded investors of approximately $65 billion by operating a fraudulent investment fund that promised consistently high returns [31]. The scheme unravelled during the financial crisis when Madoff was unable to meet redemption requests, leading to his arrest and subsequent sentencing to 150 years in prison. In the years following Madoff's conviction, the U.S. government worked to compensate victims [32]. The magnitude of the Madoff case reinforced the need for stricter oversight of investment firms and prompted increased regulatory measures to protect investors from similar schemes.

Financial fraud has not been limited to individuals; major financial institutions have also engaged in fraudulent activities, as seen in the Wells Fargo account fraud scandal. Between 2002 and 2016, Wells Fargo employees, under

pressure to meet aggressive sales targets, created millions of unauthorized bank and credit card accounts [33]. This fraudulent activity went undetected for years, causing financial harm to customers and leading to significant fines and reputational damage for the bank. The scandal highlighted systemic weaknesses in corporate governance and underscored the importance of ethical business practices within the banking sector.

The evolution of money laundering and financial fraud in the U.S. demonstrates an ongoing struggle between illicit actors and regulatory bodies. While legislative measures such as the BSA, the Money Laundering Control Act, and the Sarbanes-Oxley Act have sought to mitigate financial crime, the adaptability of fraudsters and the complicity of financial institutions continue to challenge enforcement efforts. There is a necessity for stronger oversight, enhanced compliance measures, and international cooperation to combat financial fraud and money laundering effectively.

3.2. Regulatory Landscape

3.2.1. Bank Secrecy Act, 1970

Enacted in 1970, the Bank Secrecy Act (BSA), also known as the Currency and Foreign Transactions Reporting Act, was the first major U.S. legislation designed to combat financial crimes such as money laundering and tax evasion [34]. It requires financial institutions to maintain records of significant transactions and report suspicious activities to federal authorities. Over the years, the BSA has been strengthened by amendments, including the USA Patriot Act of 2001, which expanded its scope to address terrorism financing and introduced stricter customer due diligence requirements [35].

The enforcement of the BSA has led to significant regulatory actions against financial institutions failing to comply with its provisions. For instance, in 2020, Goldman Sachs agreed to a $2.9 billion settlement over its role in the 1MDB scandal, which involved illicit financial transactions across multiple jurisdictions [36]. These cases highlight the serious consequences of non-compliance and the importance of strong anti-money laundering (AML) controls.

Key provisions of the BSA include Currency Transaction Reports (CTRs), which mandate that financial institutions report cash transactions exceeding $10,000, and Suspicious Activity Reports (SARs), which require reporting of potentially illicit transactions regardless of amount. The Act also imposes Customer Due Diligence (CDD) measures, compelling financial institutions to verify customer identities and assess risk factors. Additionally, the BSA enforces recordkeeping requirements to facilitate financial investigations and mandates information sharing between institutions and federal agencies to enhance AML efforts.

Despite its effectiveness, challenges remain. The rise of cryptocurrencies and other emerging financial technologies has created new avenues for illicit transactions, requiring continuous regulatory adaptation. International cooperation is however crucial, as financial crimes often span multiple jurisdictions, making collaboration with global AML frameworks essential.

3.3. USA Patriot Act, 2001

The USA Patriot Act was enacted in response to the September 11, 2001, terrorist attacks as a critical measure to combat money laundering and prevent the misuse of the U.S. financial system for illicit purposes [37]. One of its most significant components is Title III, officially known as the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001 [38]. This section of the law strengthens existing anti-money laundering (AML) frameworks by enhancing due diligence obligations, increasing regulatory oversight, and fostering greater cooperation between financial institutions and law enforcement agencies. The Act was designed to target not only conventional money laundering schemes but also terrorist financing networks that exploit weaknesses in financial regulations.

A key provision of the USA Patriot Act is its reinforcement of customer due diligence (CDD) measures within financial institutions. The Act mandates the implementation of comprehensive Customer Identification Programs (CIPs), requiring banks and other financial entities to verify the identities of individuals opening new accounts. This measure ensures that financial institutions assess the risk profile of their clients and mitigate potential threats of money laundering and terrorism financing. The Act also introduced more stringent Know Your Customer (KYC) requirements, compelling banks to maintain detailed records of transactions and conduct ongoing monitoring to detect suspicious financial activities.

Another critical element of the USA Patriot Act is its expansion of information-sharing mechanisms between financial institutions and government agencies. Prior to its enactment, regulatory and law enforcement agencies faced limitations in accessing financial data that could reveal illicit activities [39]. The Act significantly improved collaboration by allowing financial institutions to share information regarding potential money laundering or terrorist financing with

federal authorities under safe harbour protections. This provision enhances the ability of agencies such as the Financial Crimes Enforcement Network (FinCEN) to detect and disrupt sophisticated financial crime networks operating both domestically and internationally.

The USA Patriot Act also granted the Department of the Treasury broader authority to impose special regulatory measures on jurisdictions, institutions, or transactions that pose a primary money laundering concern. Under Section 311 of the Act, the Treasury can designate foreign financial institutions or entire countries as high-risk entities, thereby restricting their access to the U.S. financial system. These measures serve as a deterrent against banks or jurisdictions that facilitate illicit financial flows and provide an additional tool for combating global money laundering activities.

The legislation further strengthened the requirements for financial institutions to develop and implement robust AML programs. Under the Act, institutions must establish internal policies, employee training programs, and independent audit procedures to ensure compliance with federal regulations. These AML programs play a crucial role in maintaining financial transparency and preventing the exploitation of banks and other financial intermediaries for illegal purposes.

3.4. Financial Crimes Enforcement Network (FinCEN) Regulations

The Financial Crimes Enforcement Network (FinCEN), established in 1990 as a bureau of the U.S. Department of the Treasury, has a significant role in combating illicit financial activities such as money laundering, terrorist financing, and fraud. By collecting, analyzing, and disseminating financial intelligence, FinCEN supports law enforcement agencies, regulatory bodies, and international partners in identifying and preventing financial crimes [40].

A cornerstone of FinCEN's regulatory framework is the enforcement of the Bank Secrecy Act (BSA), which mandates financial institutions to comply with stringent reporting and recordkeeping obligations [41]. As noted earlier in this research, under the BSA, institutions must file Currency Transaction Reports (CTRs) for cash transactions exceeding $10,000 to deter large-scale money laundering schemes. Additionally, Suspicious Activity Reports (SARs) are required for transactions that exhibit suspicious patterns, such as structuring deposits to evade reporting thresholds or engaging with high-risk entities [42]. These reports provide law enforcement with critical intelligence to dismantle financial crime networks.

In 2016, FinCEN introduced the Customer Due Diligence (CDD) Rule, known as the "fifth pillar" of anti-money laundering (AML) compliance [43]. This rule requires financial institutions to verify the beneficial owners of legal entity customers, thereby enhancing transparency and preventing criminals from exploiting anonymous corporate structures to launder illicit funds.

FinCEN also facilitates financial intelligence sharing through Section 314 of the USA Patriot Act. Section 314(a) enables law enforcement to request information from financial institutions on individuals linked to terrorism or money laundering. Section 314(b) allows financial institutions to collaborate and share data to better detect and report suspicious activities. This framework enhances crime prevention by fostering rapid information exchange. Recognizing the rise of digital assets, FinCEN has expanded its oversight to virtual currencies [44]. In December 2020, it proposed regulations requiring banks and money service businesses to monitor transactions involving convertible virtual currencies (CVCs) or digital assets, addressing anonymity risks in digital finance [45]. Through its evolving regulations, enforcement actions, and intelligence-sharing efforts, FinCEN remains a cornerstone in protecting the U.S. financial system from illicit exploitation.

3.5. Role of Agencies like the SEC, FDIC, and OCC

Several key federal regulatory agencies engage significantly in enforcing anti-money laundering (AML) regulations and ensuring the integrity of the U.S. financial system. These agencies namely, the Securities and Exchange Commission (SEC), the Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) oversee various financial institutions and enforce compliance with the Bank Secrecy Act (BSA), the USA PATRIOT Act, and other relevant AML laws [46]. Their collective efforts help prevent financial crimes such as money laundering, fraud, and terrorist financing while promoting transparency and stability in the financial sector.

The Securities and Exchange Commission (SEC) primarily regulates the securities industry, including stock exchanges, broker-dealers, and investment advisors [47]. Given the vulnerability of capital markets to money laundering schemes and financial fraud, the SEC mandates that regulated entities establish and maintain robust AML programs. Broker-dealers, in particular, are required to comply with the BSA by implementing internal policies for detecting and reporting suspicious activities [47]. Additionally, the SEC collaborates with the Financial Industry Regulatory Authority (FINRA) to conduct examinations and enforce AML compliance within the securities industry. The SEC also investigates cases of

market manipulation, insider trading, and accounting fraud, ensuring that illicit actors do not exploit the financial markets for money laundering purposes [48].

The Federal Deposit Insurance Corporation (FDIC) plays supervisory role to state-chartered banks that are not members of the Federal Reserve System. As part of its regulatory functions, the FDIC ensures that banks adhere to AML laws, particularly the BSA and provisions of the USA PATRIOT Act [49]. Financial institutions under FDIC supervision must implement effective AML programs, conduct customer due diligence (CDD), and file Suspicious Activity Reports (SARs) when necessary. The FDIC also conducts regular examinations to assess compliance with these regulations and has the authority to impose enforcement actions, including monetary penalties and restrictions on banking operations, against institutions that fail to meet AML standards. Through these supervisory measures, the FDIC helps maintain the safety and soundness of the U.S. banking system while mitigating risks associated with money laundering and financial fraud [49].

The Office of the Comptroller of the Currency (OCC) is responsible for regulating and supervising all national banks and federal savings associations. As part of its oversight duties, the OCC ensures that these institutions comply with AML laws and regulations by conducting routine examinations and risk assessments [50]. The OCC has the authority to take enforcement actions against non-compliant institutions, including issuing cease-and-desist orders, imposing civil monetary penalties, and removing bank executives who violate AML laws. Given the role of large national banks in processing international transactions, the OCC's regulatory oversight is critical in identifying and preventing cross-border money laundering schemes [46, 50].

By working in coordination, the SEC, FDIC, and OCC help establish a strong regulatory framework that deters financial crimes and promotes accountability within the financial system. Their enforcement efforts, coupled with stringent compliance requirements for financial institutions, contribute to the overall integrity and resilience of the U.S. financial sector.

4. The role of artificial intelligence in combating money laundering and fraud

Artificial Intelligence (AI) has emerged as a transformative force in the financial sector, offering innovative solutions to longstanding challenges of money laundering and fraud. Leveraging advanced technologies like machine learning algorithms, neural networks, predictive analytics, natural language processing (NLP), and blockchain integration, financial institutions can enhance their detection and prevention mechanisms. This comprehensive analysis explores the sophisticated role of AI in combating financial crimes, supported by case studies from U.S. financial institutions.

4.1. AI-Driven Fraud Detection: Machine Learning Algorithms, Neural Networks, and Predictive Analytics

Traditional fraud detection methods often rely on rule-based systems, which can be rigid and slow to adapt to evolving fraudulent behaviours [6]. AI-driven approaches, particularly machine learning algorithms and neural networks, have revolutionized this landscape by enabling systems to learn from data and improve over time. These technologies analyze vast datasets to identify patterns and anomalies indicative of fraudulent activities [3, 5, 6]. Predictive analytics further enhances this capability by forecasting potential risks based on historical data and emerging trends [6].

For instance, AI can detect unusual transaction patterns that deviate from a customer's typical behaviour, flagging them for further investigation. This proactive stance allows for early intervention, reducing financial losses and enhancing regulatory compliance. Companies like C3 AI have developed specialized AI-driven anti-money laundering solutions that improve the accuracy of detecting suspicious activities while significantly reducing false-positive alerts. Their platform enhances investigator productivity through intelligent case recommendations and advanced visualizations of key contextual data [51].

4.2. Natural Language Processing (NLP) for Financial Crime Detection

NLP, a subset of AI, focuses on the interaction between computers and human language. In the context of financial crime detection, NLP facilitates the analysis of unstructured data sources such as emails, transaction descriptions, and social media posts [52]. Through the processing and understanding textual information, NLP can identify suspicious communications, fraudulent documentation, or indicators of collusion [52].

For example, NLP algorithms can sift through vast amounts of textual data to uncover hidden relationships between entities involved in money laundering schemes, providing deeper insights and aiding investigators [53]. This capability enhances the efficiency of compliance teams by automating the analysis of large volumes of data that would be

impractical to process manually. As financial criminals often use complex language and jargon to obscure their activities, NLP's ability to interpret and analyze natural language is invaluable in detecting and preventing financial crimes.

4.3. Blockchain and AI Integration in Financial Security

The convergence of AI and blockchain technology presents a formidable defense against financial crimes. Blockchain's decentralized and immutable ledger ensures transparency and traceability of transactions, while AI enhances the ability to analyze and interpret this data efficiently [54]. Integrating AI with blockchain allows for real-time monitoring of transactions, rapid anomaly detection, and automated compliance checks.

This synergy not only bolsters security but also streamlines operations, reducing the reliance on manual processes and minimizing human error. Financial institutions adopting this integrated approach can achieve a more robust and resilient framework against money laundering and fraud [54, 55]. AI algorithms can analyze blockchain data to identify patterns associated with fraudulent activities, such as rapid movement of funds across multiple accounts [55]. This integration enhances the ability to detect and prevent complex financial crimes that traditional systems might overlook.

4.4. Case studies of AI Applications in U.S. Financial Institutions

Several U.S. financial institutions have successfully implemented AI to combat financial crimes:

- JPMorgan Chase: The bank has integrated AI to bolster employee productivity and customer service. With 200,000 employees actively using new AI tools, JPMorgan has transformed various job functions, including client interactions and legal documentation, thereby enhancing efficiency and accuracy [56].
- Bank of America Erica Virtual Assistant: In 2018, Bank of America launched Erica, a virtual assistant powered by AI, to enhance customer service. Erica assists customers with tasks such as transaction searches, bill payments, and financial advice through voice and text interactions within the bank's mobile app [57]. By 2021, Erica had surpassed 1 billion client interactions having assisted nearly 32 million clients, demonstrating the growing acceptance and effectiveness of AI-driven customer service solutions in the banking sector [58].
- American Express Machine Learning Model for Fraud Prevention: American Express has been at the forefront of utilizing AI to combat fraud. In 2014, the company implemented large-scale machine learning models for fraud detection, resulting in a significant improvement over previous method [59]. By 2020, these AI systems were monitoring over a trillion in annual transactions, generating fraud decisions in milliseconds [60]. This proactive approach contributed to American Express maintaining the lowest fraud rates in the industry for years, with losses at half the rate of other major networks

5. Challenges and limitations of ai in anti-money laundering (aml) and fraud detection

Artificial Intelligence (AI) has significantly enhanced the detection and prevention of money laundering and fraud in financial institutions. However, AI-driven AML and fraud detection systems face critical challenges, including algorithmic bias, regulatory concerns, data privacy risks, adversarial attacks, and institutional resistance. Addressing these issues is essential to ensuring the reliability and fairness of AI-powered financial security systems.

5.1. Ethical Concerns and Bias in AI Systems

Algorithmic bias remains a major challenge in AI-driven AML systems, as models trained on historical data may reinforce discriminatory patterns [61]. Studies indicate that AI models used in financial risk assessments have flagged transactions from minority groups as high-risk at disproportionate rates [62]. A notable case occurred in 2019 when Apple’s credit card, issued by Goldman Sachs, faced scrutiny for allegedly offering lower credit limits to women despite similar financial profiles [63].

False positives in AI-driven AML systems further complicate fraud detection. As many as 95% of AML transaction monitoring alerts are false positives, costing billions in wasted investigation time, according to a 2020 report by Global Investigations Review [64]. To mitigate these issues, financial institutions must adopt fairness-aware AI models and employ explainable AI (XAI) to enhance transparency.

5.2. Limitations in AI Models and Adversarial Attacks

AI models struggle with identifying novel money laundering tactics that deviate from historical patterns. Criminals exploit these gaps through adversarial attacks, manipulating transaction data to evade detection [65]. A recent study

found that adversarial attacks reduced the accuracy of fraud detection models significantly, highlighting AI's vulnerabilities [66].

5.3. Resistance to AI Adoption

Despite AI's potential, financial institutions face hurdles in adoption due to high implementation costs, regulatory uncertainty, and skill gaps. A 2022 McKinsey survey revealed that 65% of financial institutions cited cost as the primary barrier to AI integration [67]. Additionally, a World Economic Forum report found that 50% of financial sector executives believed their workforce lacked sufficient AI expertise [68]. To overcome these challenges, financial institutions must balance AI's capabilities with ethical, regulatory, and security considerations while ensuring human oversight in fraud detection.

6. Future prospects and policy recommendations

As financial crimes continue to evolve in complexity, artificial intelligence (AI) is expected to play an even more significant role in combating money laundering and fraud. Future advancements in AI-driven financial security will focus on enhancing detection capabilities, strengthening regulatory frameworks, and fostering collaboration between public and private stakeholders to ensure a robust and secure financial system

6.1. Innovations in AI for Financial Security

The future of AI in anti-money laundering (AML) and fraud prevention will be shaped by continuous technological advancements. Key innovations include:

6.1.1. Enhanced Machine Learning Models

Future AI systems should employ more advanced deep learning techniques, such as reinforcement learning and federated learning, to improve fraud detection. These models will enable financial institutions to analyze vast amounts of data while preserving customer privacy. Federated learning, in particular, will allow multiple institutions to collaborate on AI model training without sharing sensitive data, reducing risks associated with centralized data storage.

6.1.2. AI-Powered Real-Time Transaction Monitoring

The next generation of AI-driven fraud detection systems should incorporate real-time transaction monitoring with minimal latency. Financial institutions will use AI-driven behavioural biometrics, which analyze user actions such as typing speed, mouse movements, and device usage, to detect fraudulent transactions more accurately.

6.1.3. Integration of AI with Blockchain Technology

AI and blockchain integration will provide enhanced transparency and security in financial transactions. Smart contracts powered by AI will allow for automated compliance checks and fraud prevention mechanisms. Blockchain's decentralized ledger can also be leveraged to track illicit financial activities, making it more difficult for criminals to launder money undetected.

6.1.4. Quantum Computing for Financial Crime Prevention

Quantum computing has the potential to revolutionize AI-driven fraud detection by solving complex problems that traditional computers struggle with. AI models enhanced by quantum algorithms will significantly improve predictive analytics, allowing for faster and more accurate detection of fraudulent activities. While still in its early stages, financial institutions are investing in quantum AI to stay ahead of evolving financial crimes.

6.2. Strengthening Regulatory Frameworks to Accommodate AI-Driven AML Strategies

Regulatory frameworks must evolve alongside AI advancements to ensure financial institutions can effectively use AI while remaining compliant with legal and ethical standards. Key policy recommendations include:

6.2.1. Establishing AI-Specific AML Regulations

Regulators should develop AI-specific guidelines for AML compliance, outlining clear standards for AI model transparency, data privacy, and bias mitigation. The U.S. Department of the Treasury and the Financial Crimes Enforcement Network (FinCEN) have reportedly begun drafting regulatory guidance on AI-driven financial security, emphasizing the need for interpretability and accountability in AI decision-making.

6.2.2. Implementing Explainable AI (XAI) Requirements

To address concerns about AI bias and opacity, financial institutions should be required to implement Explainable AI (XAI) techniques. XAI enables human auditors to understand how AI models make decisions, reducing the risk of false positives and ensuring fairness in fraud detection.

6.2.3. Enhancing Cross-Border AI Compliance Standards

Given the global nature of financial crimes, international cooperation is crucial. Regulatory bodies such as the Financial Action Task Force (FATF) and the International Monetary Fund (IMF) should establish unified AI-driven AML standards to facilitate cross-border collaboration and data-sharing among financial institutions.

6.2.4. Regular AI Audits and Compliance Testing

Financial institutions should be subject to regular AI audits by regulatory bodies to ensure their fraud detection systems remain effective, unbiased, and compliant with evolving laws. AI stress-testing mechanisms should be introduced to simulate real-world money laundering schemes and assess AI model resilience.

6.3. The Role of Public-Private Partnerships in Enhancing AI Applications in Financial Crime Prevention

Public-private partnerships (PPPs) are essential for aligning AI advancements with regulatory expectations while improving financial security by fostering collaboration between governments, financial institutions, and technology firms. These partnerships improve data access, drive innovation, and ensure regulatory compliance. Joint AI research initiatives, such as those by the Bank for International Settlements (BIS), enhance fraud detection through advanced analytics. Secured data-sharing frameworks allow financial institutions to strengthen AI training while maintaining compliance with privacy laws like GDPR.

Addressing AI skill gaps is also crucial. Training programs, such as those in the EU, equip compliance officers with expertise in AI fraud detection. Likewise, the global cooperation emphasized by the UNODC enables intelligence-sharing to combat AI-assisted money laundering.

7. Conclusion

The integration of artificial intelligence (AI) in combating money laundering and financial fraud represents a transformative shift in financial crime prevention. This study has explored the historical evolution of money laundering in the United States, the legal and institutional frameworks ensuring accountability, and the role of AI-driven technologies in enhancing anti-money laundering (AML) efforts. AI applications, including machine learning algorithms, natural language processing (NLP), and blockchain integration, have demonstrated significant potential in detecting suspicious activities, strengthening compliance, and reducing fraudulent transactions. However, challenges such as ethical concerns, regulatory compliance issues, and financial institutions' resistance to AI adoption remain barriers to full implementation.

The findings of this study carry profound implications for financial institutions, regulators, and policymakers. For financial institutions, AI adoption offers a more efficient and effective approach to fraud detection and risk management. However, institutions must balance innovation with compliance, ensuring that AI systems are transparent, unbiased, and aligned with legal standards. Regulators, on the other hand, face the challenge of updating and strengthening existing frameworks to accommodate AI-driven AML strategies. Regulatory bodies must establish clear guidelines for AI use in financial crime prevention while addressing concerns related to data privacy, accountability, and potential algorithmic bias. Policymakers must also prioritize the creation of legal and ethical frameworks that foster AI innovation while protecting consumers and financial markets from unintended consequences.

Conclusively, AI is poised to play an increasingly critical role in the fight against money laundering and financial fraud. While its benefits in enhancing detection capabilities and compliance efficiency are undeniable, the technology must be carefully integrated within a well-defined regulatory and ethical framework. Public-private partnerships, global collaboration, and policy reforms will be essential in maximizing AI's potential while mitigating associated risks. As financial crime tactics evolve, the adoption of AI-driven solutions will be crucial in maintaining the integrity and security of the U.S. financial system.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] Baldwin FN, Gadboys JA. The duty of financial institutions to investigate and report suspicions of Fraud, financial crime, and corruption. InFinancial crimes: Psychological, technological, and ethical Issues 2016 Jun 9 (pp. 83-104). Cham: Springer International Publishing.

[2] Dawaki FZ, Yakubu S. Combating Money Laundering in the United States: The Recent Development. UMYU Law Journal. 2021 Dec 31;2(2):181-96.

[3] Srinivasagopalan LN. AI-enhanced fraud detection in healthcare insurance: A novel approach to combatting financial losses through advanced machine learning models. European Journal of Advances in Engineering and Technology. 2022;9(8):82-91.

[4] Kute DV, Pradhan B, Shukla N, Alamri A. Deep learning and explainable artificial intelligence techniques applied for detecting money laundering–a critical review. IEEE access. 2021 Jun 4;9:82300-17.

[5] Yeoh P. Artificial intelligence: accelerator or panacea for financial crime?. Journal of Financial Crime. 2019 Apr 1;26(2):634-46.

[6] Rohit KD, Patel DB. Review on detection of suspicious transaction in anti-money laundering using data mining framework. International Journal for Innovative Research in Science & Technology. 2015;1(8):129-33.

[7] Immaneni J. Using Swarm Intelligence and Graph Databases for Real-Time Fraud Detection. Journal of Computational Innovation. 2021 Nov 15;1(1).

[8] Carta S, editor. Machine learning and the city: applications in architecture and urban design. John Wiley & Sons; 2022 Jun 7.

[9] Mahalakshmi V, Kulkarni N, Kumar KP, Kumar KS, Sree DN, Durga S. The role of implementing artificial intelligence and machine learning technologies in the financial services industry for creating competitive intelligence. Materials Today: Proceedings. 2022 Jan 1;56:2252-5.

[10] Alzubi J, Nayyar A, Kumar A. Machine learning from theory to algorithms: an overview. InJournal of physics: conference series 2018 Nov (Vol. 1142, p. 012012). IOP Publishing.

[11] Shah C, Sabbella VR, Buvvaji HV. From Deterministic to Data-Driven: AI and Machine Learning for Next-Generation Production Line Optimization. Journal of Artificial Intelligence and Big Data. 2022:21-31.

[12] Korejo MS, Rajamanickam R, Md. Said MH. The concept of money laundering: a quest for legal definition. Journal of Money Laundering Control. 2021 Oct 21;24(4):725-36.

[13] Cassella SD. Toward a new model of money laundering: Is the "placement, layering, integration" model obsolete?. Journal of Money Laundering Control. 2018 Oct 1;21(4):494-7.

[14] Reurink A. Financial fraud: A literature review. Contemporary topics in finance: A collection of literature surveys. 2019 Apr 5:79-115.

[15] Adetunji A. A Comparative Analysis of the Control of Financial Crime From the Perspective of the UK, USA and Nigeria (Doctoral dissertation, School of Advanced Study, University of London). Retrieved from: https://sas-space.sas.ac.uk/6701/ Accessed 4 December, 2022.

[16] Pooley K, Ferguson CE. Using environmental criminology theories to compare 'youth misuse of fire'across age groups in New South Wales. Australian & New Zealand Journal of Criminology. 2017 Mar;50(1):100-22.

[17] Kathuli TM. An Assessment Of The Effectiveness Of The Financial Reporting Centre And Financial Institutions In Prevention Of Money Laundering: A Case Study Of Nairobi County. 2018 (Doctoral dissertation, University of Nairobi). Retrieved from: <https://erepository.uonbi.ac.ke/handle/11295/104689> Accessed 6 December, 2022

[18] Maulidi A. When and why (honest) people commit fraudulent behaviours? Extending the fraud triangle as a predictor of fraudulent behaviours. Journal of Financial Crime. 2020 Apr 23;27(2):541-59.

[19] Awang, Naqiah & Hussin, Nur Syafiqah & Razali, Fatin & Abu Talib, Shafinaz. Fraud Triangle Theory: Calling for New Factors. Insight Journal. (2020). 7. 54-64. 10.24191/ij.v7i1.62.

[20] Scott WR. Organizational sociology. Routledge; 2016 Dec 5.

[21] Scott WR. Institutional theory: Contributing to a theoretical research program. Great minds in management: The process of theory development. 2005 Jan;37(2):460-84.

[22] Shittu AK. Advances in AI-driven credit risk models for financial services optimization. International Journal of Multidisciplinary Research and Growth Evaluation. 2022 Jan;3(1):660-76.

[23] Van Cranenburgh S, Wang S, Vij A, Pereira F, Walker J. Choice modelling in the age of machine learning-discussion paper. Journal of choice modelling. 2022 Mar 1;42:100340.

[24] Carcillo F, Le Borgne YA, Caelen O, Kessaci Y, Oblé F, Bontempi G. Combining unsupervised and supervised learning in credit card fraud detection. Information sciences. 2021 May 1;557:317-31.

[25] Owen A, Templer S. Intelligent Fraud Detection: Design a machine learning framework for real-time fraud prevention in transactions. 2022. Available at: https://www.researchgate.net/profile/Antony-Owen/publication/389250222_Intelligent_Fraud_Detection_Design_a_machine_learning_framework_for_real-time_fraud_prevention_in_transactions/links/67ba022e96e7fb48b9caaed1/Intelligent-Fraud-Detection-Design-a-machine-learning-framework-for-real-time-fraud-prevention-in-transactions.pdf Accessed 16 December, 2022.

[26] Antonopoulos GA, Papanicolaou G. Organized crime: a very short introduction. Oxford University Press; 2018.

[27] Lessambo F. The US banking system. Springer International Publishing; 2020.

[28] PBS LearningMedia. From Watergate to campaign finance reform. 2022. Available from: https://www.pbslearningmedia.org/resource/from-watergate-to-campaign-finance-reform-video/retro-report/ Accessed 16 December, 2022.

[29] Amicelle A. When finance met security: Back to the War on Drugs and the problem of dirty money. Finance and Society. 2017 Jan;3(2):106-23.

[30] Connell M. The fall of Enron and the creation of the Sarbanes-Oxley Act of 2002. Available at https://core.ac.uk/download/pdf/232014888.pdf Accessed 18 December, 2022.

[31] Azim M, Azam S. Bernard Madoff's 'Ponzi Scheme': Fraudulent behaviour and the role of auditors. Accountancy Business and the Public interest. 2016;15(1):122-37.

[32] Adams GS, Mullen E. Punishing the perpetrator decreases compensation for victims. Social Psychological and Personality Science. 2015 Jan;6(1):31-8.

[33] Shichor D, Heeren JW. Reflecting on corporate crime and control: The Wells Fargo banking saga. Journal of White Collar and Corporate Crime. 2021 Jun;2(2):97-108.

[34] Howard C. Financial crimes compliance self-governance: applying the Faragher defense to bank secrecy act/anti-money laundering violations. U. Mem. L. Rev.. 2017;48:45.

[35] Coto AS. Customer due diligence: FinCEN and the beneficial ownership requirement for legal entity customers. NC Banking Inst.. 2016;20:145.

[36] Kulamadayil L. Grand theft in international law. London Review of International Law. 2022 Nov 1;10(3):427-57.

[37] Hamm MS. The USA Patriot Act and the politics of fear. InCultural criminology unleashed 2016 Apr 15 (pp. 301-314). Routledge-Cavendish.

[38] Booysen SL. A comparative analysis of the aspects of the law of South Africa and the United States of America regarding money laundering and the financing of terrorism (Master's thesis, University of Johannesburg (South Africa)). Available at https://www.proquest.com/openview/a60a1fef2d72ad23a3cf7c727df7d29a/1?cbl=2026366&diss=y&pq-origsite=gscholar Accessed 16 December, 2022.

[39] Santucci L. Can Data Sharing Help Financial Institutions Improve the Financial Health of Older Americans?. FRB of Philadelphia Payment Cards Center Discussion Paper. 2017 Nov(17-1).

[40] Holovkin B, Marysyuk K. Foreign experience in countering (preventing) organized crime in the financial system: special law enforcement bodies and strategic priorities. Baltic Journal of Economic Studies. 2019;5(3):25-36.

[41] Hughes SJ, Middlebrook ST. Advancing a framework for regulating cryptocurrency payments intermediaries. Yale J. on Reg.. 2015;32:495.

[42] També Bearpark N. Case Studies and Empirical Findings. InDeconstructing Money Laundering Risk: De-risking, the Risk-based Approach and Risk Communication 2022 Jul 15 (pp. 89-142). Cham: Springer International Publishing.

[43] Silvia JE. The Fifth Pillar and FinCEN's New Rules on Customer Due Diligence. Banking LJ. 2017;134:57.

[44] Toscher S, Stein MR. Cryptocurrency-FinCEN and Discovery of Hidden Wealth. J. Tax Prac. & Proc.. 2018;20:19.

[45] Cohen L, Angelovska-Wilson A, Strong G, Law D. Decentralized finance: Ready for its "close-up"?. GLI–Blockchain & Cryptocurrency Regulation 2022. 2021 Oct.

[46] Harper DC. Protecting financial services while ensuring regulatory compliance. Utica College; 2016.

[47] Poser NS. Reflections on the Securities Broker as a Fiduciary. SMUL Rev.. 2015;68:845.

[48] Golumbic, Court E.. The big chill: personal liability and the targeting of financial sector compliance officers. Hastings LJ. 2017;69:45.

[49] Hogan TL, Johnson K. Alternatives to the federal deposit insurance corporation. The Independent Review. 2016 Jan 1;20(3):433-54.

[50] Menand L. Why Supervise Banks? The Foundations of the American Monetary Settlement. Vand. L. Rev.. 2021;74:951.

[51] C3 AI Available at: https://c3.ai/products/c3-ai-anti-money-laundering/?utm_source= Accessed 22 December, 2022.

[52] Dash B. Information Extraction from Unstructured Big Data: A Case Study of Deep Natural Language Processing in Fintech. University of the Cumberlands; 2022.

[53] Datta A, Sujay D, Shandilya SK. Introduction to Cyber Crime Investigation: A Modern Approach. InAdvancements in Cyber Crime Investigations and Modern Data Analytics (pp. 1-15). CRC Press.

[54] Nassar M, Salah K, Ur Rehman MH, Svetinovic D. Blockchain for explainable and trustworthy artificial intelligence. Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery. 2020 Jan;10(1):e1340.

[55] Salah K, Rehman MH, Nizamuddin N, Al-Fuqaha A. Blockchain for AI: Review and open research challenges. IEEE access. 2019 Jan 1;7:10127-49.

[56] Allayannis GY, Becker JM. A global FinTech overview. Darden Case No. UVA-F-1860. 2019 Apr 26.

[57] Kochhar K, Purohit H, Chutani R. The rise of artificial intelligence in banking sector. InThe 5th international conference on educational research and practice (icerp) 2019 (Vol. 127).

[58] Bank of America. Bank of America's Erica tops 1 billion client interactions, now assists nearly 32 million clients. 2022 Oct 24 [cited 22 December, 2022]. Available from: https://newsroom.bankofamerica.com/content/newsroom/press-releases/2022/10/bank-of-america-s-erica-tops-1-billion-client-interactions--now-.html

[59] Cohen MC. Big data and service operations. Production and Operations Management. 2018 Sep;27(9):1709-23.

[60] Damlapinar M. Analytics of Life: Making Sense of Artificial Intelligence, Machine Learning and Data Analytics. NLITX; 2019 Nov 11.

[61] SHUKLA N, ALAMRI A. Deep Learning and Explainable Artificial Intelligence Techniques Applied for Detecting Money Laundering–A Critical Review.

[62] Rovatsos M, Mittelstadt B, Koene A. Landscape summary: Bias in algorithmic decision-making: What is bias in algorithmic decision-making, how can we identify it, and how can we mitigate it?. Available at https://www.research.ed.ac.uk/en/publications/landscape-summary-bias-in-algorithmic-decision-making-what-is-bia Accessed 22 December, 2022.

[63] ABC News. Apple Card algorithm accused of gender discrimination [Internet]. 2019 Nov 12. Available from: https://www.abc.net.au/news/2019-11-12/apple-card-algorithm-accused-of-gender-discrimination/11696160 Accessed 22 December, 2022.

[64] Blackdot Solutions. Reducing false positives in AML transaction monitoring [Internet]. 2020. Available from: https://blackdotsolutions.com/blog/aml-alerts/ Accessed 22 December, 2022.

[65] Li D, Li Q. Adversarial deep ensemble: Evasion attacks and defenses for malware detection. IEEE Transactions on Information Forensics and Security. 2020 Jun 19;15:3886-900.

[66] Iyer N. Adversarial Machine Learning: Exploring Security Vulnerabilities in AI-Driven Systems. International Journal of Artificial Intelligence, Data Science, and Machine Learning. 2022;3(1):1-9.

[67] McKinsey & Company. The state of AI in 2022—and a half decade in review [Internet]. 2022 Dec 6. Available from: https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2022-and-a-half-decade-in-review Accessed 22 December, 2022.

[68] World Economic Forum. The Future of Jobs Report 2022 [Internet]. Geneva: World Economic Forum; 2022. Available from: https://www3.weforum.org/docs/WEF_Future_of_Jobs_2022.pdf Accessed 22 December, 2022.