**Financial Risk Management in Digital-Only Banks: Addressing Fraud and Cybersecurity Threats in a Cashless Economy**

**Abstract**

*This study examines financial risk management in digital-only banking by analyzing fraud and cybersecurity threats using quantitative methodologies. Leveraging Verizon’s Data Breach Investigations Report (2024), the European Central Bank Cyber Resilience Oversight Report (2023), and the Financial Action Task Force Money Laundering & Fraud Prevention Report (2024), this research employs descriptive statistics, logistic regression, and Difference-in-Differences (DiD) analysis to assess fraud risks, cybersecurity framework effectiveness, and regulatory impact. Results indicate that phishing (35%) and ransomware (20%) account for the highest financial losses, averaging $5.5M and $7.1M per incident, respectively. Logistic regression confirms that Basel III compliance reduces fraud risks (-70.759 coefficient), while AI-driven fraud monitoring shows inefficiencies (21.918 coefficient). Regulatory enforcement leads to a 1.90% greater fraud reduction in strictly regulated banks. Recommendations include enhanced AI fraud detection, stricter compliance enforcement, multi-layered security measures, and targeted fraud awareness programs to strengthen digital banking resilience.*

**Keywords: Digital-Only Banking, Fraud Detection, Cybersecurity Risks, Regulatory Compliance, Financial Risk Management**

### **1. Introduction**

The rise of digital-only banks has significantly reshaped financial services by enhancing accessibility and efficiency through technology-driven solutions. Operating without physical branches, these institutions facilitate cashless transactions, streamline banking operations, and improve customer experience. However, their reliance on digital infrastructure increases exposure to financial risks, particularly fraud and cybersecurity threats, necessitating comprehensive risk management strategies to maintain consumer trust and institutional stability (George et al., 2024).

According to Global Market Insights (2024), the expansion of digital banking has been remarkable, with the market valued at approximately $10.9 trillion in 2023 and projected to maintain a compound annual growth rate (CAGR) exceeding 3% between 2024 and 2032. Adoption has also surged, with an estimated 1.75 billion registered accounts globally processing transactions totaling $1.4 trillion annually (Pham, 2024). Mobile banking applications have become the dominant mode of financial transactions, particularly among younger demographics, with 60% of Millennials, 57% of Generation Z, and 52% of Generation X preferring digital banking platforms (American Bankers Association, 2023). Despite these advantages, increased reliance on digital banking has led to growing cybersecurity threats, fraudulent activities, and regulatory compliance challenges, necessitating enhanced security frameworks to address evolving risks (Oyewole et al., 2024).

Financial fraud and cybersecurity breaches have had profound implications for digital-only banks. IBM (2024) states that in 2024, financial institutions experienced an average data breach loss of approximately $5.9 million, underscoring the severity of financial vulnerabilities within the sector. Additionally, 23% of all global phishing attacks in 2023 targeted financial institutions, illustrating the persistent threat of cybercrime (Husain, 2025). The absence of consistent consumer protection policies exacerbates these risks. Report indicate that certain banks in the United Kingdom reimbursed less than 10% of fraud-related financial losses in 2022, emphasizing the need for more effective fraud mitigation strategies (Quinio, 2024).

Several high-profile incidents illustrate the susceptibility of digital-only banks to cyber threats. In October 2024, the United Kingdom’s Financial Conduct Authority (FCA) imposed a £29 million fine on Starling Bank due to deficiencies in financial crime controls (Quinio & Arnold, 2024). Despite prior regulatory warnings, the bank struggled with anti-money laundering (AML) and sanctions compliance, resulting in substantial penalties. This case highlights the necessity for stringent AML frameworks in digital banking (Internationalbanker, 2021). Similarly, in June 2024, Evolve Bank & Trust, a key partner for fintech firms such as Affirm and Wise, suffered a data breach orchestrated by the cybercrime group LockBit, exposing sensitive customer data and causing operational disruptions (Rapa, 2024). In September 2024, the bank further compounded its security challenges by freezing over $100 million in customer funds, preventing fintech clients from accessing their accounts (Ekhator, 2024). These incidents underscore the importance of robust cybersecurity protocols and transparent crisis management strategies.

Beyond individual cases, systemic financial risks have raised broader concerns. According to Patag (2022), Banco de Oro (BDO) Unibank in Southeast Asia suffered a major hacking incident between November and December 2021, where over 700 account holders reported unauthorized fund transfers executed without standard security measures such as one-time passwords (OTPs). This breach revealed significant security vulnerabilities and reinforced the need for multi-layered fraud detection mechanisms. Similarly, Revolut has faced ongoing security concerns. In 2024, customers reported substantial financial losses due to inadequate identity verification processes, with one individual losing €197,000 within an hour and another defrauded of €67,000 in minutes (Blancaro, 2024). Weak customer support and delayed responses to fraudulent activities exacerbated reputational damage, demonstrating the consequences of ineffective fraud prevention strategies.

Regulatory oversight has played a crucial role in addressing financial risks within digital banking. Ozioko 2024) posits that regulatory intervention has been essential in mitigating financial crime risks and enforcing compliance. N26, a German fintech company, faced restrictions from BaFin due to AML compliance concerns, limiting new customer registrations to 50,000 per month (FintechGlobal, 2024). However, following substantial improvements in fraud prevention measures, these restrictions were lifted in 2024, allowing the bank to expand its customer base. This case illustrates the importance of regulatory compliance in maintaining financial stability (Partington, 2024). Additionally, historical cyberattacks, such as the Tesco Bank hack in 2016 and the Carbanak and Cobalt cyberattacks between 2014 and 2016, demonstrated the sophistication of malware threats targeting financial institutions (Financial Conduct Authority, 2018). More recently, Revolut suffered a data breach in 2022 attributed to internal security failures, reinforcing the risks posed by insider threats and inadequate cybersecurity controls.

As cyber threats become increasingly complex, digital banks must prioritize cybersecurity as an essential component of their risk management strategies. According to Banking Exchange Staff (2023), a survey of Chief Risk Officers in banking revealed that 72% identified cybersecurity as the most critical risk factor for the year ahead. Additionally, research suggests that human error contributes to 88% of cybersecurity breaches, underscoring the necessity of comprehensive employee training programs and robust internal security protocols (Sikder, 2017; Burrell, 2024). Financial institutions have responded by increasing investments in risk management technologies. According to PricewaterhouseCoopers (2022), in 2022, 41% of banking institutions planned to expand their risk management budgets by up to 10%, while an additional 24% projected increases exceeding this threshold.

To combat financial fraud and cybersecurity threats, regulatory bodies and financial institutions have introduced frameworks aimed at strengthening digital banking security. The European Central Bank (ECB) and the Federal Financial Institutions Examination Council (FFIEC) have established cybersecurity guidelines designed to enhance resilience within the financial sector. Reports from cybersecurity firms, such as Verizon’s Data Breach Investigations Report (DBIR) and IBM’s X-Force Threat Intelligence Index, provide valuable insights into the evolving cyber threats confronting financial institutions (Vericon, 2024; Xantrion Cybersecurity, 2024). To mitigate risks, digital banks are increasingly leveraging artificial intelligence (AI) and machine learning (ML) in fraud detection and risk assessment. AI-powered analytics facilitate real-time fraud monitoring, while ML algorithms continuously adapt to emerging cyber threats. Additionally, emerging technologies such as blockchain and biometric authentication are being explored to strengthen fraud prevention and customer verification processes (Chatterjee et al., 2024).

Maintaining consumer trust remains a critical challenge for digital-only banks. While a survey by Americans Bankers Association (2023) found that 87% of bank customers believe their financial institutions take proactive measures to protect them from fraud, cases such as those involving Revolut and BDO Unibank demonstrate how ineffective fraud response mechanisms can weaken consumer confidence. This research is highly relevant to the scientific community as it provides a comprehensive analysis of financial risk management in digital-only banking, a rapidly growing sector in the modern financial landscape. By employing advanced quantitative techniques such as logistic regression and Difference-in-Differences (DiD) analysis, the study offers valuable insights into fraud detection, cybersecurity threats, and regulatory compliance. The findings contribute to both academic research and practical applications, assisting financial institutions and policymakers in strengthening risk mitigation strategies. Ultimately, this research enhances the understanding of digital banking vulnerabilities and fosters the development of more resilient financial security frameworks. This research aims to analyze and evaluate financial risk management strategies in digital-only banks, focusing on addressing fraud and cybersecurity threats in a cashless economy, with the goal of identifying effective risk mitigation frameworks and regulatory measures that enhance financial security and consumer trust, by achieving the following objectives:

1. To examine the key financial risks associated with digital-only banking, particularly in the areas of fraud and cybersecurity threats.
2. To analyze existing fraud detection and cybersecurity frameworks used by digital-only banks and assess their effectiveness.
3. To evaluate the impact of regulatory compliance and risk management policies on mitigating financial fraud and cybersecurity risks in digital banking.
4. To propose strategic recommendations for enhancing financial risk management in digital-only banks, incorporating emerging technologies and regulatory best practices.

### **2. Literature Review**

Financial risk management in digital banking relies on several theoretical frameworks that address both conventional financial risks and emerging cybersecurity threats. According to Wisista and Noveria (2023), the Modern Portfolio Theory (MPT), introduced by Harry Markowitz in 1952, emphasizes diversification to optimize the risk-return trade-off. While originally applied to investment portfolios, its principles extend to digital banking by encouraging diversification in asset holdings and revenue streams to mitigate market volatility (Mwania, 2023; Balogun, 2025). However, critics argue that MPT’s reliance on market efficiency and normally distributed returns may not fully apply to digital banking, where technological disruptions and cyber risks create unpredictable financial conditions (Letho et al., 2022; Ngware, 2021; Kolade et al., 2025; Balogun, et al., 2025).

The Basel Accords, established by the Basel Committee on Banking Supervision, serve as a regulatory foundation for banking risk management (Hasan & Suzuki, 2021; Balogun et al., 2025). Basel I set minimum capital requirements to address credit risk, while Basel II introduced supervisory reviews and market discipline mechanisms (Gopalakrishnan et al., 2021; Obioha-Val, 2025). In response to the 2008 financial crisis, Basel III strengthened capital adequacy, stress testing, and liquidity requirements (Tamplin, 2023; Olutimehin, 2025). For digital banks, adherence to Basel III mandates the maintenance of sufficient capital buffers to absorb losses from cyber incidents and fraud (Birindelli et al., 2022; Obioha-Val et al., 2025). However, the rapid evolution of digital financial services complicates regulatory adaptation, underscoring the need for flexible, technology-responsive frameworks (Obeng et al., 2024; Obioha-Val et al., 2025).

Enterprise Risk Management (ERM) provides a comprehensive approach to risk assessment by integrating financial, operational, strategic, and reputational risks. In digital banking, ERM frameworks are essential for addressing cybersecurity threats and fraud by fostering a risk-aware culture and embedding risk considerations into decision-making (Ononiwu et al., 2024; Obioha-Val et al., 2025). According to ACCA (2023), the Committee of Sponsoring Organizations of the Treadway Commission (COSO) asserts that ERM enhances organizational resilience by ensuring continuous risk assessment and mitigation. However, maintaining an effective ERM system requires significant resources and constant vigilance against evolving threats (Ahmad et al., 2023; Olutimehin, 2025).

From a cybersecurity perspective, the Cyber Kill Chain model, developed by Lockheed Martin, offers a structured methodology for identifying and mitigating cyberattacks (Kareem et al., 2024; Olutimehin et al., 2025). It outlines attack stages from reconnaissance to data exfiltration, allowing digital banks to implement targeted security measures. However, its linear structure may not fully capture the complexity of modern cyber threats, which often involve multiple, overlapping attack vectors (Mahboubi et al., 2024; Olutimehin, 2025). In contrast, the Zero Trust Security model operates on the principle of "never trust, always verify," requiring continuous authentication and authorization for all users and devices (Khan, 2023; Alao et al., 2024). While Zero Trust enhances security by minimizing unauthorized access, it presents challenges in balancing security with user experience.

The Fraud Triangle Theory further explains financial crime by identifying three elements: opportunity, pressure, and rationalization (Mandal & S, 2023; Val et al., 2024). In digital banking, the ease of online transactions and user anonymity create opportunities for fraud, while financial pressures, such as personal debt, can drive individuals toward fraudulent activities. According to Chhabra Roy and P (2024), rationalization further enables perpetrators to justify their actions. Digital banks mitigate these risks through stringent internal controls, continuous monitoring, and ethical training programs. However, critics argue that the Fraud Triangle oversimplifies financial crime by neglecting factors such as organizational culture and leadership (Maulidi, 2024; Bhat & Kolhe, 2024; Salako et al., 2024).

### **Digital-Only Banking: Evolution, Growth, and Risk**

### The transition from traditional branch-based banking to digital-only platforms has been driven by technological advancements, evolving consumer behavior, and regulatory developments. According to Kumar (2023), this shift began in the 1960s with the introduction of mainframe computers automating banking functions, followed by the launch of Automated Teller Machines (ATMs) in 1967, which provided customers with continuous access to cash and account services. The commercialization of the internet in the 1990s further accelerated this transition, with Wells Fargo pioneering online banking in 1995 (Gupta, 2024; Olateju et al., 2024). By the early 2000s, the widespread adoption of smartphones and mobile applications enabled the emergence of digital-only banks that operate without physical branches (Ionașcu et al., 2023; Samuel-Okon et al., 2024).

### The global digital banking market has expanded significantly, valued at approximately $10.9 trillion in 2023 and projected to reach $15.4 trillion by 2032, with a compound annual growth rate (CAGR) exceeding 3% (Global Market Insights, 2024). Consumer demand for speed, accessibility, and convenience has been a primary driver of this growth. According to American Bankers Association (2023), 64% of Generation Z and 68% of Millennials primarily use mobile banking applications, while 55% of Generation X also favor mobile platforms. Although Baby Boomers show lower adoption rates, with 41% preferring desktop-based online banking, overall digital banking adoption has increased across all age groups, particularly following the COVID-19 pandemic, which reinforced the necessity of remote financial services (MXTechnologies, 2025).

### Despite its advantages, digital-only banking presents substantial risks, particularly in cybersecurity and fraud prevention. Teichmann and Boticiu (2024) asserts that identity theft, account takeovers, and phishing scams remain significant concerns, with the financial sector experiencing an average data breach cost of $5.9 million in 2024 (ABA, 2024; Gbadebo et al., 2024). Additionally, phishing attacks accounted for over 23% of cyber threats targeting financial institutions in 2023, underscoring the sector’s vulnerability (Ghosh & Sil, 2024; Joseph, 2024). The growing sophistication of ransomware and malware attacks has resulted in major financial losses and operational disruptions. A notable example is the June 2024 breach at Evolve Bank & Trust, where the cybercrime group LockBit compromised sensitive customer data, affecting corporate fintech clients and raising concerns about digital banking security (Rapa, 2024; Farrington, 2024).

### The reliance on third-party fintech providers further compounds operational risks. Many digital-only banks integrate external services for payment processing, customer onboarding, and fraud detection, introducing security vulnerabilities (Stalmachova et al., 2022; Mayeke et al., 2024). Regulatory frameworks such as the Basel Accords and the Payment Services Directive 2 (PSD2) aim to address these risks by enforcing security standards and fostering competition in financial services (Barbereau et al., 2024; Kolade et al., 2024). However, ensuring compliance with evolving regulations remains a challenge, requiring continuous oversight and adaptive security measures (Shandilya et al., 2024; Adigwe et al., 2024).

### **Table 1: Financial Risks in Digital-Only Banks: Key Risks, References, and Case Studies**

|  |  |  |
| --- | --- | --- |
| **Key Financial Risks in Digital-Only Banks** | **References (Credible Sources)** | **Case Studies** |
| **Phishing Attacks** | Verizon’s 2023 Data Breach Investigations Report (DBIR) | 23% of all global phishing attacks targeted financial institutions in 2023 (IBM) |
| **Data Breaches** | IBM X-Force Threat Intelligence Index 2024 | Evolve Bank & Trust breach in June 2024 exposed customer data |
| **Ransomware Attacks** | Aon Global Risk Management Survey 2023 | Starling Bank fined £29M in 2024 for financial crime control failures |
| **Insider Fraud** | Association of Certified Fraud Examiners (ACFE) 2024 | Revolut customers lost €197,000 and €67,000 in identity fraud cases (2024) |
| **Money Laundering** | Financial Action Task Force (FATF) 2023 Report | N26 faced AML compliance restrictions from BaFin until 2024 |
| **API Vulnerabilities** | Open Web Application Security Project (OWASP) API Security 2024 | Tesco Bank hack in 2016 resulted in £2.5 million stolen from customers |

### **Fraud in Digital-Only Banks: Trends, Tactics, and Challenges**

The rise of digital-only banks has transformed financial services, introducing both opportunities and vulnerabilities, particularly in fraud prevention and detection. According to Chatterjee et al. (2024), identity fraud remains one of the most pervasive threats, encompassing both traditional identity theft and synthetic identity fraud. Traditional identity theft involves unauthorized access to personal information to obtain financial services fraudulently, whereas synthetic identity fraud combines real and fabricated data to create fictitious identities (Mungai, 2024; Okon et al., 2024). The latter is particularly difficult to detect, as no single victim typically reports suspicious activity. Additionally, payment fraud—such as unauthorized transactions and chargebacks—exploits weaknesses in digital banking systems, resulting in financial losses for institutions and consumers (Beju & Făt, 2023; Olabanji et al., 2024). Money laundering and terrorist financing risks have also escalated, as digital banking’s anonymity enables illicit fund transfers, complicating regulatory compliance efforts (Saxena, 2024; Olabanji et al., 2024).

Emerging fraudulent tactics demonstrate the adaptability of cybercriminals to technological advancements. Social engineering schemes, including phishing and vishing, have evolved to incorporate deepfake fraud, where artificial intelligence convincingly mimics individuals’ voices and images to deceive authentication systems (Schmitt & Flechais, 2024; Ajayi et al., 2025). The growing sophistication of deepfake technology threatens digital identity verification, enabling fraudsters to bypass security protocols. Furthermore, Tamraparani (2025) posits that automated fraud attacks leveraging artificial intelligence allow perpetrators to execute large-scale fraudulent activities efficiently. Insider threats further exacerbate risks, as employees with privileged access to sensitive information may engage in fraudulent activities, either independently or in collusion with external actors. The Association of Certified Fraud Examiners (ACFE) underscores the importance of stringent internal controls and fostering an ethical corporate culture to mitigate these risks (Idrus et al., 2024; Oladoyinbo et al., 2024).

Detecting and preventing fraud in digital-only banks presents significant challenges. Traditional rule-based fraud detection systems often struggle to keep pace with rapidly evolving fraudulent tactics (Olushola & Mart, 2024; Olabanji et al., 2024). The necessity for real-time transaction monitoring in a high-volume digital environment requires advanced analytical tools capable of identifying anomalies without disrupting legitimate transactions. However, many consumers resist additional security measures, such as multi-factor authentication and biometric verification, citing inconvenience. According to Brito and Abuzneid (2024) that ease of access is a primary concern for consumers, often outweighing security considerations, which complicates the implementation of stricter authentication measures.

Addressing fraud in digital banking necessitates a multifaceted approach integrating advanced technological solutions, stringent internal controls, and consumer education. Enhancing fraud detection through artificial intelligence and machine learning, strengthening regulatory compliance, and fostering collaboration between financial institutions and regulatory agencies are critical to safeguarding digital banking operations against evolving threats (Balakrishnan, 2024; Olaniyi et al., 2023).

### **Cybersecurity Threats in Digital Banking**

### Digital-only banks, while improving accessibility and efficiency in financial services, face escalating cybersecurity threats that compromise operational integrity and customer trust. According to Shah et al. (2022), one of the most significant threats is Distributed Denial-of-Service (DDoS) attacks, which flood banking systems with excessive traffic, disrupting services for legitimate users. Often driven by geopolitical tensions and hacktivist activities, these attacks target financial institutions due to their critical infrastructure. Another major concern is ransomware, where malicious software encrypts banking data, forcing institutions to pay a ransom for restoration (Ryan, 2021; Olaniyi et al., 2024). Such attacks lead to financial losses, operational disruptions, and regulatory scrutiny (George et al., 2024). Application Programming Interface (API) vulnerabilities present additional risks. As digital banks increasingly integrate third-party fintech services, undocumented or misconfigured APIs expand attack surfaces, increasing exposure to data breaches and unauthorized access. The Open Web Application Security Project (OWASP) emphasizes that robust authentication, authorization, and data validation measures are essential to mitigate these threats (Chahal et al., 2022).

### Several high-profile breaches illustrate these cybersecurity challenges. In October 2024, Starling Bank was fined £29 million by the UK’s Financial Conduct Authority for failing to implement adequate financial crime controls, increasing its exposure to money laundering and fraud (Quinio & Arnold, 2024). Similarly, in 2024, Evolve Bank & Trust suffered a breach compromising the personal and financial data of 7.6 million customers, exacerbated by its dependence on third-party fintech providers (Rapa, 2024). Earlier cases, such as the 2016 Tesco Bank cyberattack, which resulted in £2.5 million in customer losses (Financial Conduct Authority, 2018), and the 2021 Banco de Oro Unibank breach, where unauthorized transactions drained accounts, demonstrate the severity of cyber intrusions (Patag, 2022). More recently, Revolut faced security lapses in 2024, with multiple customers reporting unauthorized transactions (Blancaro, 2024).

### To mitigate these threats, digital banks deploy multi-layered cybersecurity defenses, including firewalls, intrusion detection systems, and anti-malware tools. Biometric authentication and behavioral analytics enhance fraud detection and identity verification. Artificial intelligence (AI) and machine learning (ML) further strengthen cybersecurity frameworks by enabling real-time threat detection. However, implementing these technologies presents challenges, including data privacy concerns, false positives, and high investment costs. Given the evolving complexity of cyber threats, digital banks must continuously adapt security measures.

### **Consumer Trust and Digital Banking Security**

Financial fraud in digital-only banks has significantly impacted consumer confidence, with case studies illustrating the severe consequences of such incidents. According to Mohammed (2024), in 2023, Livia Firth's sustainability consultancy lost £324,634 to an invoice scam, leading to insolvency after an 11-month legal battle to recover the funds. Similarly, a 76-year-old man lost his life savings of $142,500 due to unauthorized transfers from his Chase bank account, a situation worsened by the bank’s initial refusal to acknowledge the fraud (Price, 2025). These cases underscore the necessity of effective fraud prevention mechanisms and responsive customer support in maintaining consumer trust.

Empirical data further highlights the erosion of trust caused by financial fraud. Mouka, (2024) asserted that 63% of respondents had either fallen victim to cyber scams or knew someone who had, leading to diminished confidence in digital banking platforms. Security concerns remain a significant barrier to adoption, particularly among older demographics who express apprehension about the safety of their funds and personal data (Li et al., 2021). This skepticism not only deters potential users but also complicates financial institutions’ efforts to foster long-term customer relationships (Sikka & Bhayana, 2024).

Customer education and fraud awareness programs have emerged as critical tools for mitigating these risks. Digital literacy empowers consumers to recognize fraud tactics such as phishing and social engineering. According to Burke et al. (2022), it has been observed that brief online educational interventions significantly reduce individuals’ susceptibility to fraud. Financial institutions have implemented interactive training modules, simulated phishing exercises, and personalized security alerts to enhance consumer awareness (Chowdhary et al., 2024). However, these programs must be tailored to different demographics and delivered through accessible channels to maximize their effectiveness (Evans et al., 2022).

Restoring consumer trust requires a multifaceted approach beyond education. Transparent communication during fraud incidents is essential, as banks that openly disclose security breaches retain customer confidence more effectively than those that obscure such events. Additionally, robust consumer protection policies and fair financial compensation frameworks are critical. The UK's £85,000 cap on fraud reimbursement has faced criticism for inadequately covering victims, highlighting the need for stronger compensation policies (Hurley, 2024). Ongoing debates continue regarding the balance between consumer responsibility and bank liability, with increasing calls for greater institutional accountability in fraud prevention (Ridzuan et al., 2024; Găbudeanu et al., 2021; Akinsola, 2025).

### **3. Methodology**

This study employs a quantitative approach using descriptive statistics, logistic regression, and difference-in-differences (DiD) analysis to assess fraud risks, cybersecurity frameworks, and regulatory impact in digital-only banking. Data sources include Verizon’s Data Breach Investigations Report (DBIR) 2024, European Central Bank (ECB) Cyber Resilience Oversight Report 2023, and Financial Action Task Force (FATF) Money Laundering & Fraud Prevention Report 2024.

Fraud risks are analyzed using descriptive statistics, calculating mean occurrence, variance, and Poisson probability to estimate fraud likelihood (Table 2). Cybersecurity framework effectiveness is evaluated via logistic regression, modeling the probability of fraud occurrence against cybersecurity measures. Regulatory impact is assessed using DiD estimation, comparing fraud incidence before and after AML policy implementation across treatment and control groups.

To ensure robustness, heteroskedasticity-consistent standard errors and Variance Inflation Factors (VIFs) are computed to test model reliability. Statistical significance is determined via the Wald test, and computational efficiency is ensured using Python (statsmodels, scikit-learn) and R (lmtest, sandwich packages).

#### **Table 2: Mathematical Formulations Used in the Study**

|  |  |  |
| --- | --- | --- |
| Analysis Type | Formula | Description |
| Mean Fraud Occurrence | $$μ=\frac{\sum\_{i=1}^{n}X\_{i}}{n}​​$$ | Average fraud cases per bank |
| Variance | $$σ^{2}= \frac{\sum\_{i=1}^{n}(X\_{i}- μ)\^2}{n} $$ | Dispersion of fraud cases |
| Poisson Probability | $$P\left(X=k\right)=\frac{λ^{k}e^{-λ}}{K!}​$$ | Probability of fraud occurrence |
| Logistic Regression | $P\left(Y=1\right)=\frac{1}{\left(1+e-^{\left(β\_{0}​+∑β\_{i}​X\_{i}\right)}\right)}​$​ | Probability of fraud based on security measures |
| Wald Test | $$Z=\frac{β^{\^}}{SE(β\^​)}​​$$ | Tests statistical significance of fraud predictors |
| Difference-in-Differences (DiD) | $$ΔY=\left(Y\_{T,post}​-Y\_{T,pre}​\right)-\left(Y\_{C,post}​-Y\_{C,pre}​\right)$$ | Fraud rate difference before and after regulation |
| Variance Inflation Factor (VIF) | $$VIF=\frac{1}{\left(1-R^{2}\right)}​$$ | Detects multicollinearity in regression |

Fraud trends, regulatory impact, and security framework effectiveness are visualized through statistical modeling and graphical representation.

1. **Results and Discussion**

**Result**

**Key Risks in Digital-Only Banking**

Digital-only banks are transforming the financial landscape by offering seamless, technology-driven banking experiences. However, their reliance on digital platforms exposes them to fraud and cybersecurity risks, making risk identification crucial for effective financial risk management. This report analyzes key threats faced by digital-only banks, highlighting their frequency, financial impact, and emerging trends.

Cybersecurity threats in digital-only banks manifest in multiple forms, including phishing, unauthorized access, ransomware, insider fraud, and API vulnerabilities. The frequency distribution of these risks, along with their financial impact, is presented in Table 3.

#### **Fraud Incidence and Financial Impact**

#### **Table 3: Distribution of Cybersecurity Threats and Financial Losses in Digital-Only Banks**

|  |  |  |  |
| --- | --- | --- | --- |
| Breach Type | Frequency (%) | Average Financial Loss per Breach ($M) | Variance in Financial Loss ($M²) |
| Phishing/Social Engineering | 35 | 5.5 | 0.367 |
| Unauthorized Access | 25 | 6.2 | 0.367 |
| Ransomware | 20 | 7.1 | 0.367 |
| Insider Threats | 10 | 5.8 | 0.367 |
| API Vulnerabilities | 10 | 6.0 | 0.367 |

Phishing and social engineering attacks emerge as the most prevalent, accounting for 35% of breaches in digital-only banks, with an average financial loss of $5.5 million per incident. Unauthorized access follows at 25%, contributing to $6.2 million in average financial damages per breach. While ransomware accounts for only 20% of breaches, it has the highest financial impact, averaging $7.1 million per incident.



#### **Figure 1: Fraud Type Distribution in Digital-Only Banks (Radar Chart)**

A moderate variance (0.367) in financial loss across breach types suggests that while digital-only banks experience different types of attacks, their financial consequences remain relatively consistent. This reinforces the need for a comprehensive risk management strategy to address multiple threats rather than focusing solely on one type of attack.

The visual representation of fraud distribution (Figure 1) confirms that phishing remains the dominant risk, followed by unauthorized access and ransomware. The radar chart effectively illustrates the comparative weight of these threats, emphasizing areas requiring enhanced security measures.

#### **Emerging Fraud Trends in Digital-Only Banks**



#### **Figure 2: Fraud Risk Representation by Financial Impact (Dot Matrix Chart)**

The rapid advancement of cybercrime techniques demands adaptive security frameworks. The dot matrix visualization (Figure 2) presents fraud risk clusters based on financial impact, demonstrating how ransomware and unauthorized access pose the most substantial financial threats. The clustering effect in Figure 2 shows a higher concentration of fraud risks at the $6 million to $7 million range, underscoring their significant financial impact.

The human element remains a critical factor in financial fraud. Over 68% of fraud incidents involve insider negligence or manipulation, reinforcing the need for advanced fraud detection technologies and employee training programs to mitigate risks.

These findings indicate that phishing attacks and unauthorized access are the most frequently occurring cybersecurity risks, while ransomware leads to the highest financial damage.

## **Fraud Detection and Cybersecurity Frameworks**

This report evaluates the impact of cybersecurity measures, AI-powered fraud monitoring, multi-factor authentication (MFA), and regulatory compliance on fraud prevention in digital banking.

#### **Table 4: Logistic Regression Results for Cybersecurity and Fraud Prevention**

|  |  |  |
| --- | --- | --- |
| Variable | Coefficient | P-Value |
| Constant | 44.552 | 1.000 |
| Cybersecurity Framework Score | 0.047 | 0.685 |
| Compliance with Basel III | -70.759 | 1.000 |
| AI-Powered Fraud Monitoring | 21.918 | 1.000 |
| Multi-Factor Authentication (MFA) | -23.461 | 1.000 |

The relationship between cybersecurity frameworks and fraud occurrence was analyzed using logistic regression modeling. The coefficients and statistical significance of each factor influencing fraud prevention are summarized in Table 4.

#### **Effectiveness of Cybersecurity Measures**

Findings suggest that Basel III compliance has the most substantial effect on reducing fraud occurrence, with a negative coefficient (-70.759), indicating that banks adhering to Basel III regulations are significantly less likely to experience fraud. However, the large coefficient value suggests possible multicollinearity with other factors.

Similarly, multi-factor authentication (MFA) shows a negative coefficient (-23.461), reinforcing its role in reducing fraud risks. Despite this, the model does not provide strong statistical evidence to confirm its effectiveness, as indicated by the p-value of 1.000.

Conversely, AI-powered fraud monitoring displays a positive coefficient (21.918), which appears counterintuitive. While AI systems are designed to detect fraud, their effectiveness may depend on implementation quality and real-time response mechanisms.



**Figure 3: Parallel Coordinates Plot of Cybersecurity Measures and Fraud Risk**

The parallel coordinates plot (Figure 3) visualizes the relationships between these cybersecurity measures and fraud occurrence. It highlights that higher cybersecurity framework scores and regulatory compliance are generally associated with lower fraud risks, whereas inconsistent AI deployment may contribute to ineffective fraud detection strategies.



#### **Figure 4: Lollipop Chart of Cybersecurity Framework Effects on Fraud Prevention**

The lollipop chart (Figure 4) further illustrates the coefficient values, making it clear that Basel III compliance and MFA implementation have the strongest negative effects on fraud occurrence. In contrast, AI-powered fraud monitoring exhibits an unexpected positive coefficient, warranting further investigation into its real-world effectiveness.

The results indicate that regulatory compliance (Basel III) and multi-factor authentication are strongly linked to reduced fraud risks, emphasizing their importance in fraud prevention strategies. However, the unexpectedly high coefficient for AI-powered fraud monitoring suggests that digital-only banks may struggle with AI model optimization or face challenges in real-time fraud detection.

## **Regulatory Impact on Fraud Mitigation**

Regulations play a critical role in financial risk management by establishing compliance frameworks that mitigate fraud and cybersecurity threats. Digital-only banks, due to their reliance on online transactions, are particularly susceptible to financial crimes such as money laundering, identity fraud, and unauthorized access. This report examines how anti-money laundering (AML) policies and regulatory compliance measures influence fraud reduction in digital banking environments.

The impact of regulatory enforcement was evaluated using a Difference-in-Differences (DiD) analysis, comparing fraud rates before and after regulatory interventions in strictly regulated and leniently regulated banking environments. The results, presented in Table 5, highlight the effectiveness of regulatory measures in reducing fraud risks in digital banks.

#### **Table 5: Difference-in-Differences (DiD) Analysis of Regulatory Impact on Fraud Reduction**

|  |  |  |  |
| --- | --- | --- | --- |
| Group | Before Regulation Avg Fraud Rate (%) | After Regulation Avg Fraud Rate (%) | Change in Fraud Rate (%) |
| Strict Regulation | 5.88 | 3.40 | -2.48 |
| Lenient Regulation | 8.24 | 7.66 | -0.58 |
| Difference-in-Differences (DiD) | NaN | NaN | -1.90 |

#### **Effectiveness of Regulatory Compliance**

Strictly regulated digital banks experienced an average fraud rate reduction of 2.48 percentage points, compared to only 0.58 percentage points in leniently regulated banks. The DiD estimate of -1.90 suggests that regulatory enforcement significantly lowers fraud rates, reinforcing the importance of stringent AML policies.



#### **Figure 5: Slope Chart of Fraud Rate Reduction Before and After Regulation**

The slope chart (Figure 5) visually represents these trends, demonstrating a steeper decline in fraud rates among strictly regulated banks, emphasizing the effectiveness of regulatory measures in financial risk mitigation.



#### **Figure 6: Dumbbell Chart Showing Fraud Rate Change Across Regulatory Environments**

The dumbbell chart (Figure 6) further emphasizes the regulatory effect by connecting before-and-after fraud rates with a clear visual representation of the reduction gap, showcasing that stricter regulatory environments lead to stronger fraud prevention outcomes.

These findings confirm that regulatory compliance significantly impacts fraud reduction, with stricter regulations leading to better fraud prevention outcomes.

**Discussion**

The findings of this study highlight the critical vulnerabilities associated with digital-only banking, reinforcing the necessity for sophisticated risk management frameworks to mitigate financial fraud and cybersecurity threats. Digital-only banks face heightened exposure to phishing, unauthorized access, ransomware, insider fraud, and API vulnerabilities, with phishing emerging as the predominant threat. The significant frequency of phishing attacks aligns with prior research emphasizing social engineering as a persistent financial risk factor in digital banking (Oyewole et al., 2024). The observed high financial impact of ransomware, despite its relatively lower frequency, supports earlier assertions that ransomware attacks are evolving in complexity, leading to severe financial consequences for financial institutions (IBM, 2024). Given the moderate variance in financial losses across breach types, the findings indicate that while threat distribution may vary, the overall financial damage remains a pressing concern, necessitating a comprehensive, multi-layered cybersecurity strategy rather than a siloed approach targeting specific threats (Burrell, 2024).

The analysis further underscores the fundamental role of cybersecurity frameworks and fraud detection mechanisms in safeguarding digital banking operations. While compliance with Basel III regulations significantly correlates with lower fraud occurrence, the presence of multicollinearity suggests that multiple security measures may be interdependent, requiring integrated cybersecurity policies for enhanced fraud prevention (Hasan & Suzuki, 2021). The observed negative relationship between multi-factor authentication (MFA) and fraud occurrence is consistent with previous research advocating for MFA as a critical fraud prevention mechanism in digital banking (Khan, 2023). However, the absence of strong statistical significance in the logistic regression model implies potential implementation inefficiencies or inconsistent enforcement of MFA policies, which may diminish its overall effectiveness. The counterintuitive positive coefficient observed for AI-powered fraud monitoring suggests that while AI is a widely adopted fraud detection tool, its effectiveness is highly contingent on deployment quality and adaptive learning capabilities. Prior studies have identified challenges in AI-driven fraud detection, including false positives, adversarial attacks, and data quality issues, which may account for the observed limitations in its predictive power (Schmitt & Flechais, 2024). This finding raises concerns regarding the reliance on AI without adequate oversight, indicating a need for continuous refinement and monitoring of machine learning models to enhance their fraud detection accuracy.

The role of regulatory frameworks in financial risk mitigation is further reinforced by the findings of the Difference-in-Differences analysis, which demonstrates a substantial reduction in fraud rates among strictly regulated digital banks. The 2.48 percentage point reduction in fraud rates post-regulation within strictly regulated environments is significantly greater than the 0.58 percentage point reduction observed in leniently regulated banks. This aligns with prior research emphasizing the importance of anti-money laundering (AML) policies and regulatory oversight in fraud mitigation (Ozioko, 2024). The observed -1.90 DiD estimate suggests that regulatory enforcement generates measurable fraud reduction benefits, reinforcing the necessity for continuous regulatory adaptation in response to evolving cyber threats (Partington, 2024). The visual representation of these findings further confirms that stricter regulatory oversight fosters enhanced financial security, reducing fraud risks more effectively than lenient regulatory environments. The steep decline in fraud rates among strictly regulated banks, as depicted in the slope chart, underscores the tangible impact of policy enforcement in financial crime prevention. The dumbbell chart further illustrates the comparative advantage of regulatory stringency in minimizing financial fraud exposure.

These findings collectively emphasize that financial risk management in digital banking must incorporate a holistic approach integrating advanced fraud detection technologies, multi-factor authentication, regulatory compliance, and adaptive machine learning-driven fraud monitoring. The significant fraud reduction in strictly regulated banks highlights the necessity of mandatory compliance with international regulatory frameworks, such as Basel III and AML directives, to ensure digital banking security (Tamplin, 2023). However, the challenges associated with AI-powered fraud monitoring signal the need for enhanced oversight in AI implementation, requiring a balance between automation and human intervention in fraud detection processes. The role of human error, accounting for over 68% of fraud incidents, further supports prior research advocating for extensive employee training programs to strengthen internal security protocols (Sikder, 2017). As digital banking continues to expand, financial institutions must prioritize a multi-faceted cybersecurity strategy encompassing not only technological advancements but also regulatory alignment and risk-aware organizational culture to sustain consumer trust and operational stability (Banking Exchange Staff, 2023).

**5. Conclusion and Recommendation**

This study underscores the pressing need for robust financial risk management strategies in digital-only banking, given the increasing incidence of fraud and cybersecurity threats. Findings reveal that phishing and ransomware attacks remain dominant, while compliance with regulatory frameworks such as Basel III and AML policies significantly mitigates fraud risks. Artificial Intelligence (AI) is vital for fraud detection in digital-only banks but faces challenges like adversarial attacks, false positives, and limited real-time learning. Logistic regression results highlight its inefficiencies, as fraudsters constantly evolve tactics, making static AI models less effective. Machine learning algorithms also struggle with imbalanced datasets, leading to biased predictions. To improve AI-driven fraud monitoring, digital banks should adopt real-time anomaly detection, continuous model training, and human oversight to minimize false alarms and enhance fraud prevention. However, inconsistencies in AI-powered fraud detection highlight implementation challenges, necessitating enhanced oversight and adaptive security measures. Strengthening digital banking security requires a multi-pronged approach integrating technological, regulatory, and operational controls to ensure financial stability and consumer trust.

1. Enhance AI-Powered Fraud Detection Systems by implementing continuous model optimization and real-time anomaly detection to improve fraud prevention accuracy.
2. Mandate Regulatory Compliance through stricter enforcement of AML policies, Basel III standards, and real-time auditing mechanisms to prevent financial crimes.
3. Adopt Multi-Layered Security Measures, including biometric authentication, behavioral analytics, and robust API security to safeguard digital banking transactions.
4. Implement Comprehensive Employee and Consumer Education Programs to mitigate human-related vulnerabilities and strengthen fraud awareness within digital banking ecosystems.

Disclaimer (Artificial intelligence)

Option 1:

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.

Option 2:

Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology

Details of the AI usage are given below:

1.

2.

3.

**References**

ABA. (2024). *Report: Average data breach cost for financial sector tops $6M*. ABA Banking Journal. <https://bankingjournal.aba.com/2024/08/report-average-data-breach-cost-for-financial-sector-tops-6m/>

ACCA. (2023). *COSO’s enterprise risk management framework | ACCA Global*. Www.accaglobal.com. <https://www.accaglobal.com/gb/en/student/exam-support-resources/professional-exams-study-resources/strategic-business-leader/technical-articles/coso-enterprise-risk-management-framework.html>

Adigwe, C. S., Mayeke, N. R., Olabanji, S. O., Okunleye, O. J., Joeaneke, P. C., & Olaniyi, O. O. (2024). The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks. *Asian Journal of Economics, Business and Accounting*, *24*(3), 289–306. <https://doi.org/10.9734/ajeba/2024/v24i31287>

Ahmad, A. S., Abdul Hamid, M., & Wahab, S. (2023). The Seven Strategic Imperative Of Enterprise Risk Management (ERM) Implementation In Financial Institutions. *International Journal of Academic Research in Business and Social Sciences*, *13*(12). <https://doi.org/10.6007/ijarbss/v13-i12/19732>

Ajayi, A. J., Joseph, S. A., Metibemu, O. C., Olutimehin, A. T., Balogun, A. Y., & Olaniyi, O. O. (2025). The Impact of Artificial Intelligence on Cyber Security in Digital Currency Transactions. *Archives of Current Research International*, *25*(2), 329–351. <https://doi.org/10.9734/acri/2025/v25i21090>

Akinsola, K. (2025). The Evolving Role of Corporate Governance in Shaping Business Practices and Legal Accountability in the 21st Century. *SSRN*. <https://doi.org/10.2139/ssrn.5115523>

Alao, A. I., Adebiyi, O. O., & Olaniyi, O. O. (2024). The Interconnectedness of Earnings Management, Corporate Governance Failures, and Global Economic Stability: A Critical Examination of the Impact of Earnings Manipulation on Financial Crises and Investor Trust in Global Markets. *Asian Journal of Economics Business and Accounting*, *24*(11), 47–73. <https://doi.org/10.9734/ajeba/2024/v24i111542>

American Bankers Association. (2023). *Consumer Survey Banking Methods 2023*. Www.aba.com. <https://www.aba.com/about-us/press-room/press-releases/consumer-survey-banking-methods-2023>

Americans Bankers Association. (2023). *Consumer Survey Digital Banking Experience 2023*. Www.aba.com. <https://www.aba.com/about-us/press-room/press-releases/consumer-survey-digital-banking-experience-2023>

Balakrishnan, A. (2024). *Leveraging Artificial Intelligence for Enhancing Regulatory Compliance in the Financial Sector*. Ssrn.com. <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4842699>

Balogun, A. Y. (2025). Strengthening Compliance with Data Privacy Regulations in U.S. Healthcare Cybersecurity. *Asian Journal of Research in Computer Science*, *18*(1), 154–173. <https://doi.org/10.9734/ajrcos/2025/v18i1555>

Balogun, A. Y., Metibemu, O. C., Olutimehin, A. T., Ajayi, A. J., Babarinde, D. C., & Olaniyi, O. O. (2025). The Ethical and Legal Implications of Shadow AI in Sensitive Industries: A Focus on Healthcare, Finance and Education. *Journal of Engineering Research and Reports*, *27*(3), 1–22. <https://doi.org/10.9734/jerr/2025/v27i31414>

Balogun, A. Y., Olaniyi, O. O., Olisa, A. O., Gbadebo, M. O., & Chinye, N. C. (2025). Enhancing Incident Response Strategies in U.S. Healthcare Cybersecurity. *Journal of Engineering Research and Reports*, *27*(2), 114–135. <https://doi.org/10.9734/jerr/2025/v27i21399>

Banking Exchange Staff. (2023). *Cyber Tops Bank Risk List for 2023: EY - Banking Exchange*. Bankingexchange.com; Banking Exchange. <https://www.bankingexchange.com/news-feed/item/9528-cyber-tops-bank-risk-list-for-2023-ey>

Barbereau, T., Weigl, L., & Pocher, N. (2024). Financial Regulation, Political Context, and Technology in the European Union. *Financial Innovation and Technology*, 19–46. <https://doi.org/10.1007/978-3-031-66047-4_2>

Beju, D.-G., & Făt, C.-M. (2023). Frauds in Banking System: Frauds with Cards and Their Associated Services. *Contributions to Finance and Accounting*, 31–52. <https://doi.org/10.1007/978-3-031-34082-6_2>

Bhat, A. H., & Kolhe, D. (2024). Crime and Fraud at Community level: Social Networking Understanding into Economic Crimes and Psychology Motivations. *Journal of Social Sciences and Economics*, *3*(2), 127–146. <https://doi.org/10.61363/g0kb2s44>

Birindelli, G., Ferretti, P., Ferri, G., & Savioli, M. (2022). Regulatory reform and banking diversity: reassessing Basel 3. *Annals of Finance*, *18*. <https://doi.org/10.1007/s10436-021-00406-3>

Blancaro, E. (2024). *Revolut Faces Scrutiny Over Record Fraud Complaints Amid Security Concerns*. The Financial Analyst. <https://thefinancialanalyst.net/2024/10/14/revolut-faces-scrutiny-over-record-fraud-complaints-amid-security-concerns/>

Brito, D., & Abuzneid, S. (2024). Multi-Factor Authentication for Keyless Entry Systems: An Innovative Approach to Automotive Security. *Journal of Information Security*, *16*(01), 78–100. <https://doi.org/10.4236/jis.2025.161004>

Burke, J., Kieffer, C., Mottola, G., & Perez-Arce, F. (2022). Can educational interventions reduce susceptibility to financial fraud? *Journal of Economic Behavior & Organization*, *198*, 250–266. <https://doi.org/10.1016/j.jebo.2022.03.028>

Burrell, D. N. (2024). Understanding Healthcare Cybersecurity Risk Management Complexity. *Revista Academiei Forţelor Terestre*, *29*(1), 38–49. <https://doi.org/10.2478/raft-2024-0004>

Chahal, N. S., Bali, P., & Khosla, P. K. (2022). A Proactive Approach to assess web application security through the integration of security tools in a Security Orchestration Platform. *Computers & Security*, *122*, 102886. <https://doi.org/10.1016/j.cose.2022.102886>

Chatterjee, P., Das, D., & Rawat, D. B. (2024). Digital twin for credit card fraud detection: Opportunities, challenges, and fraud detection advancements. *Future Generation Computer Systems*, *158*. <https://doi.org/10.1016/j.future.2024.04.057>

Chhabra Roy, N., & P, S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance*, *26*(6). <https://doi.org/10.1108/dprg-02-2024-0029>

Chowdhary, S. K., Kumar, P., Mittal, R., Gumber, I., Jangra, V., & Srivastava, P. (2024). Phishing detection tool for financial emails. *International Journal of Financial Engineering*, *11*(4). <https://doi.org/10.1142/s2424786324420027>

Ekhator, O. (2024). *Court extends freezing order on 818 accounts linked to ₦10 billion cyberattack on Hope PSBank*. Techpoint Africa. <https://techpoint.africa/2024/10/15/court-extends-freezing-order-hope-psbank/>

Evans, W. D., Abroms, L. C., Broniatowski, D., Napolitano, M., Arnold, J., Ichimiya, M., & Agha, S. (2022). Digital Media for Behavior Change: Review of an Emerging Field of Study. *International Journal of Environmental Research and Public Health*, *19*(15), 9129. <https://doi.org/10.3390/ijerph19159129>

Farrington, R. (2024). *The College Investor*. The College Investor. <https://thecollegeinvestor.com/46977/evolve-bank-trust-hit-by-ransomware-attack/>

Financial Conduct Authority. (2018). *FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack*. FCA. <https://www.fca.org.uk/news/press-releases/fca-fines-tesco-bank-failures-2016-cyber-attack>

FintechGlobal. (2024). *N26 fined €9.2m by BaFin for late money laundering reports*. FinTech Global. <https://fintech.global/2024/05/23/n26-fined-e9-2m-by-bafin-for-late-money-laundering-reports/>

Găbudeanu, L., Brici , I., Codruța Mare, C., Mihai, I. C., & Șcheau, M. C. (2021). Privacy Intrusiveness in Financial-Banking Fraud Detection. *ProQuest*, *9*(6), 104. <https://doi.org/10.3390/risks9060104>

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., & Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. *Journal of Engineering Research and Reports*, *26*(11), 7–27. <https://doi.org/10.9734/jerr/2024/v26i111311>

George, A. S., Baskar, T., & Srikaanth, P. B. (2024). Cyber Threats to Critical Infrastructure: Assessing Vulnerabilities Across Key Sectors. *Partners Universal International Innovation Journal*, *2*(1), 51–75. <https://doi.org/10.5281/zenodo.10639463>

Ghosh, B., & Sil, R. (2024). Analysis of Cyber Risk in Finance: The State-of-the-Art and Future Research Trends. *Springer Geography*, 385–400. <https://doi.org/10.1007/978-3-031-77596-3_17>

Global Market Insights. (2024a). *Digital Banking Market Size - By Banking (Retail, Corporate, Investment), Service (Transactional, Non-Transactional), Mode (Online Banking Platforms, Mobile Banking Apps), End Users (Individuals, Government Organizations, Corporates) & Forecast, 2024 - 2032*. Global Market Insights, Inc. <https://www.gminsights.com/industry-analysis/digital-banking-market>

Global Market Insights. (2024b). *Digital Banking Market Trends | Global Share Forecast Report 2026*. Global Market Insights, Inc. <https://www.gminsights.com/industry-analysis/digital-banking-market>

Gopalakrishnan, B., Jacob, J., & Mohapatra, S. (2021). Risk-sensitive Basel regulations and firms’ access to credit: Direct and indirect effects. *Journal of Banking & Finance*, *126*, 106101. <https://doi.org/10.1016/j.jbankfin.2021.106101>

Gupta, N. (2024). Fintech: Evolution, Trends, and Directions. *in Utilizing Technology for Sustainable Resource Management Solutions, IGI Global*, 232–247. <https://doi.org/10.4018/979-8-3693-2346-5.ch015>

Hasan, A. K. M. K., & Suzuki, Y. (2021). *Implementation of Basel Accords in Bangladesh*. Springer Singapore. <https://doi.org/10.1007/978-981-16-3472-7>

Hurley, F. (2024). *UK Lowers Bank Fraud Coverage Cap to £85K, Impacting Economy and Investors*. The Financial Analyst. <https://thefinancialanalyst.net/2024/09/03/uk-lowers-bank-fraud-coverage-cap-to-85k-impacting-economy-and-investors/>

Husain, O. (2025). *99 Global Phishing Statistics & Industry Trends (2023–2025)*. Control D Blog. <https://controld.com/blog/phishing-statistics-industry-trends/>

IBM. (2024, July). *Cost of a Data Breach 2024*. IBM; IBM. <https://www.ibm.com/reports/data-breach>

Idrus, M., Adriana, N., Rustam, A., Sulistyowati, N. W., & Rewa, K. A. (2024). The Impact of Forensic Accounting on Financial Fraud Prevention: A Comparative Analysis Across Countries. *the Journal of Academic Science.*, *1*(8), 1074–1084. <https://doi.org/10.59613/m6jrt421>

Internationalbanker. (2021). *The Top Challenges in Anti-Money Laundering and Sanctions Compliance*. International Banker. <https://internationalbanker.com/finance/the-top-challenges-in-anti-money-laundering-and-sanctions-compliance/>

Ionașcu, A. E., Gheorghiu, G., Spătariu, E. C., Munteanu, I., Grigorescu, A., & Dănilă, A. (2023). Unraveling Digital Transformation in Banking: Evidence from Romania. *Systems*, *11*(11), 534. <https://doi.org/10.3390/systems11110534>

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. <https://doi.org/10.9734/jerr/2024/v26i91271>

Kareem, K., Naik, N., Jenkins, P., Grace, P., & Song, J. (2024). Understanding the Defence of Operational Technology (OT) Systems: A Comparison of Lockheed Martin’s Cyber Kill Chain, MITRE ATT&CK Framework, and Diamond Model. *Lecture Notes in Networks and Systems*, *884*, 605–624. <https://doi.org/10.1007/978-3-031-74443-3_35>

Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105–116. <https://doi.org/10.30574/wjarr.2023.19.3.1785>

Kolade, T. M., Aideyan, N. T., Oyekunle, S. M., Ogungbemi, O. S., & Olaniyi, O. O. (2024). Artificial Intelligence and Information Governance: Strengthening Global Security, through Compliance Frameworks, and Data Security. *Asian Journal of Research in Computer Science*, *17*(12), 36–57. <https://doi.org/10.9734/ajrcos/2024/v17i12528>

Kolade, T. M., Obioha-Val, O. A., Balogun, A. Y., Gbadebo, M. O., & Olaniyi, O. O. (2025). AI-Driven Open Source Intelligence in Cyber Defense: A Double-edged Sword for National Security. *Asian Journal of Research in Computer Science*, *18*(1), 133–153. <https://doi.org/10.9734/ajrcos/2025/v18i1554>

Kumar, V. (2023). Fintech. *Management for Professionals*, 111–229. <https://doi.org/10.1007/978-981-19-8148-7_2>

Letho, L., Chelwa, G., & Alhassan, A. L. (2022). Cryptocurrencies and portfolio diversification in an emerging market. *China Finance Review International*, *12*(1), 20–50. <https://doi.org/10.1108/cfri-06-2021-0123>

Li, W., Yigitcanlar, T., Erol, I., & Liu, A. (2021). Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science*, *80*(1), 102211. <https://doi.org/10.1016/j.erss.2021.102211>

Mahboubi, A., Luong, K., Aboutorab, H., Bui, H. T., Jarrad, G., Bahutair, M., Camtepe, S., Pogrebna, G., Ahmed, E., Barry, B., & Gately, H. (2024). Evolving techniques in cyber threat hunting: A systematic review. *Journal of Network and Computer Applications*, *232*, 104004–104004. <https://doi.org/10.1016/j.jnca.2024.104004>

Mandal, A., & S, A. (2023). Fathoming fraud: unveiling theories, investigating pathways and combating fraud. *Journal of Financial Crime*, *31*(5). <https://doi.org/10.1108/jfc-06-2023-0153>

Maulidi, A. (2024). The enigma of fraud as a unique crime and its resonance for auditing research and practice: unlearned lessons of psychological pathways to fraud. *Journal of Accounting & Organizational Change*, *21*(1). <https://doi.org/10.1108/jaoc-04-2023-0076>

Mayeke, N. R., Arigbabu, A. T., Olaniyi, O. O., Okunleye, O. J., & Adigwe, C. S. (2024). Evolving Access Control Paradigms: A Comprehensive Multi-Dimensional Analysis of Security Risks and System Assurance in Cyber Engineering. *Asian Journal of Research in Computer Science*, *17*(5), 108–124. <https://doi.org/10.9734/ajrcos/2024/v17i5442>

Mohammed, H. (2024). *Livia Firth‘s Eco-age Closes After Being “Targeted by Criminals.”* WWD. <https://wwd.com/sustainability/business/livia-firths-eco-age-closes-down-1236512000/>

Mouka, M. (2024). *Cyber scams fuel distrust in digital payments, Chubb report finds | bobsguide*. Bobsguide. <https://www.bobsguide.com/cyber-scams-fuel-distrust-in-digital-payments-chubb-report-finds/>

Mungai, R. (2024). Synthetic Identity Fraud a Critical Primary National Security Priority. *Social Science Research Network*. <https://doi.org/10.2139/ssrn.4770398>

Mwania, E. K. (2023). Effect of Portfolio Diversification on the Financial Performance of Listed Investment Firms in East Africa: a Comparative Analysis Across the Pre-, During, and Post Covid-19 Period. *Uonbi.ac.ke*. <http://erepository.uonbi.ac.ke/handle/11295/166375>

MXTechnologies. (2025). *Modern Banking Experiences for Gen Z & Millennials*. Mx.com. <https://www.mx.com/research/genz-millennial-banking-perspectives/>

Ngware, S. G. (2021). Banks’ Portfolio Diversification on Financial Performance of Commercial Banks in Kenya. *Jkuat.ac.ke*. <http://localhost/xmlui/handle/123456789/5640>

Obeng, S., Iyelolu, V., Adewale, A., & Idemudia, C. (2024). The Transformative Impact of Financial Technology (FinTech) on Regulatory Compliance in the Banking Sector. *World Journal of Advanced Research and Reviews*, *23*(1), 2008–2018. <https://doi.org/10.30574/wjarr.2024.23.1.2184>

Obioha-Val, O. A. (2025). Bridging Gaps in Cybersecurity Governance: Leveraging Collaborative Digital Solutions. *Asian Journal of Research in Computer Science*, *18*(2), 82–100. <https://doi.org/10.9734/ajrcos/2025/v18i2564>

Obioha-Val, O. A., Gbadebo, M. O., Olaniyi, O. O., Chinye, N. C., & Balogun, A. Y. (2025). Innovative Regulation of Open Source Intelligence and Deepfakes AI in Managing Public Trust. *Journal of Engineering Research and Reports*, *27*(2), 136–156. <https://doi.org/10.9734/jerr/2025/v27i21400>

Obioha-Val, O. A., Lawal, T. I., Olaniyi, O. O., Gbadebo, M. O., & Olisa, A. O. (2025). Investigating the Feasibility and Risks of Leveraging Artificial Intelligence and Open Source Intelligence to Manage Predictive Cyber Threat Models. *Journal of Engineering Research and Reports*, *27*(2), 10–28. <https://doi.org/10.9734/jerr/2025/v27i21390>

Obioha-Val, O. A., Olaniyi, O. O., Gbadebo, M. O., Balogun, A. Y., & Olisa, A. O. (2025). Cyber Espionage in the Age of Artificial Intelligence: A Comparative Study of State-Sponsored Campaign. *Asian Journal of Research in Computer Science*, *18*(1), 184–204. <https://doi.org/10.9734/ajrcos/2025/v18i1557>

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., & Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. <https://doi.org/10.9734/jerr/2024/v26i91269>

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., & Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. <https://doi.org/10.9734/ajrcos/2024/v17i3424>

Olabanji, S. O., Olaniyi, O. O., & Olagbaju, O. O. (2024). Leveraging Artificial Intelligence (AI) and Blockchain for Enhanced Tax Compliance and Revenue Generation in Public Finance. *Asian Journal of Economics, Business and Accounting*, *24*(11), 577–587. <https://doi.org/10.9734/ajeba/2024/v24i111577>

Olabanji, S. O., Oluwaseun Oladeji Olaniyi, O. O., & Olaoye, O. O. (2024). Transforming Tax Compliance with Machine Learning: Reducing Fraud and Enhancing Revenue Collection. *Asian Journal of Economics Business and Accounting*, *24*(11), 503–513. <https://doi.org/10.9734/ajeba/2024/v24i111572>

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., & Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. <https://doi.org/10.9734/ajarr/2024/v18i2601>

Olaniyi, O. O., Okunleye, O. J., & Olabanji, S. O. (2023). Advancing Data-Driven Decision-Making in Smart Cities through Big Data Analytics: A Comprehensive Review of Existing Literature. *Current Journal of Applied Science and Technology*, *42*(25), 10–18. <https://doi.org/10.9734/cjast/2023/v42i254181>

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., & Oladoyinbo, T. O. (2024). CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 32. <https://doi.org/10.9734/JERR/2024/v26i61160>

Olateju, O. O., Okon, S. U., Olaniyi, O. O., Samuel-Okon, A. D., & Asonze, C. U. (2024). Exploring the Concept of Explainable AI and Developing Information Governance Standards for Enhancing Trust and Transparency in Handling Customer Data. *Journal of Engineering Research and Reports*, *26*(7), 244–268. <https://doi.org/10.9734/jerr/2024/v26i71206>

Olushola, A., & Mart, J. (2024). Fraud Detection using Machine Learning. *ScienceOpen*. <https://doi.org/10.14293/pr2199.000647.v1>

Olutimehin, A. T. (2025a). Advancing Cloud Security in Digital Finance: AI-Driven Threat Detection, Cryptographic Solutions, and Privacy Challenges. *Journal of Engineering Research and Reports*, *27*(3), 35–55. <https://doi.org/10.9734/jerr/2025/v27i31416>

Olutimehin, A. T. (2025b). Assessing the Effectiveness of Cybersecurity Frameworks in Mitigating Cyberattacks in the Banking Sector and its Applicability to Decentralized Finance (DeFi). *Asian Journal of Research in Computer Science*, *18*(3), 130–151. <https://doi.org/10.9734/ajrcos/2025/v18i3583>

Olutimehin, A. T. (2025c). The Synergistic Role of Machine Learning, Deep Learning, and Reinforcement Learning in Strengthening Cyber Security Measures for Crypto Currency Platforms. *Asian Journal of Research in Computer Science*, *18*(3), 190–212. <https://doi.org/10.9734/ajrcos/2025/v18i3586>

Olutimehin, A. T., Ajayi, A. J., Metibemu, O. C., Balogun, A. Y., Oladoyinbo, T. O., & Olaniyi, O. O. (2025). Adversarial Threats to AI-Driven Systems: Exploring the Attack Surface of Machine Learning Models and Countermeasures. *Journal of Engineering Research and Reports*, *27*(2), 341–362. <https://doi.org/10.9734/jerr/2025/v27i21413>

Ononiwu, M. I., Onwuzulike, O. C., Shitu, K., & Ojo, O. O. (2024). Operational risk management in emerging markets: A case study of Nigerian banking institutions. *World Journal of Advanced Research and Reviews*, *23*(3), 446–459. <https://doi.org/10.30574/wjarr.2024.23.3.2705>

Oyewole, A. T., Okoye, C. C., Ofodile, O. C., & Ugochukwu, C. E. (2024). Cybersecurity risks in online banking: A detailed review and preventive strategies applicatio. *World Journal of Advanced Research and Reviews*, *21*(3), 625–643. <https://doi.org/10.30574/wjarr.2024.21.3.0707>

Ozioko, A. C. (2024). Preventive Strategies for Financial Institutions: Compliance and Legal Implications. *Multi-Disciplinary Research and Development Journals Int’l*, *5*(1), 86–107. <http://mdrdji.org/index.php/mdj/article/view/87>

Partington, M. (2024). *N26 growth limits lifted by German financial regulator | Sifted*. Sifted. <https://sifted.eu/articles/germany-n26-neobank-regulator-news>

Patag, K. J. (2022). *Four indicted over massive hacking of BDO accounts*. Philstar.com. <https://www.philstar.com/business/2022/01/26/2156516/four-indicted-over-massive-hacking-bdo-accounts>

Pham, M. (2024). *Developing Telecoms*. Developing Telecoms. <https://developingtelecoms.com/telecom-technology/financial-services/16452-gsma-records-1-75-billion-mobile-money-accounts.html>

Price, K. (2025). *Scammers stole his $142K life savings. He says his bank didn’t protect him.* Nj. <https://www.nj.com/news/2025/02/scammers-stole-his-142k-life-savings-he-says-his-bank-didnt-protect-him.html>

PricewaterhouseCoopers. (2022). *Banking on growth, but challenged to manage risks in a new coordinated way*. PwC. <https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey/banking-capital-markets-risk.html>

Quinio, A. (2024). *Some UK banks fully refund fraud losses in less than 10% of cases, says regulator*. @FinancialTimes; Financial Times. <https://www.ft.com/content/5d3c23d4-b772-4f0e-af91-2d8632784af6>

Quinio, A., & Arnold, M. (2024). *Starling Bank fined £29mn over “shockingly lax” crime controls*. @FinancialTimes; Financial Times. <https://www.ft.com/content/a19b4073-8de1-4dbb-9df7-092a6db9025e>

Rapa, A. (2024). *Client alert: Incident highlights the hidden dangers of third-party relationships for fintech firms*. WTW. <https://www.wtwco.com/en-us/insights/2024/07/client-alert-incident-highlights-the-hidden-dangers-of-third-party-relationships-for-fintech-firms>

Ridzuan, N. N., Masri, M., Anshari, M., Fitriyani, N. L., & Syafrudin, M. (2024). AI in the Financial Sector: The Line between Innovation, Regulation and Ethical Responsibility. *Information*, *15*(8), 432. <https://doi.org/10.3390/info15080432>

Ryan, M. W. (2021). Ransomware Revolution: The Rise of a Prodigious Cyber Threat. In *Advances in information security*. Springer New York. <https://doi.org/10.1007/978-3-030-66583-8>

Salako, A. O., Fabuyi, J. A., Aideyan, N. T., Selesi-Aina, O., Dapo-Oyewole, D. L., & Olaniyi, O. O. (2024). Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance. *Asian Journal of Research in Computer Science*, *17*(12), 66–88. <https://doi.org/10.9734/ajrcos/2024/v17i12530>

Samuel-Okon, A. D., Akinola, O. I., Olaniyi, O. O., Olateju, O. O., & Ajayi, S. A. (2024). Assessing the Effectiveness of Network Security Tools in Mitigating the Impact of Deepfakes AI on Public Trust in Media. *Archives of Current Research International*, *24*(6), 355–375. <https://doi.org/10.9734/acri/2024/v24i6794>

Saxena, C. (2024). Identifying transaction laundering red flags and strategies for risk mitigation. *Journal of Money Laundering Control*, *27*(6), 1063–1077. <https://doi.org/10.1108/jmlc-11-2023-0182>

Schmitt, M., & Flechais, I. (2024). Digital deception: generative artificial intelligence in social engineering and phishing. *Artificial Intelligence Review*, *57*(12). <https://doi.org/10.1007/s10462-024-10973-2>

Shah, Z., Ullah, I., Li, H., Levula, A., & Khurshid, K. (2022). Blockchain Based Solutions to Mitigate Distributed Denial of Service (DDoS) Attacks in the Internet of Things (IoT): A Survey. *Sensors*, *22*(3), 1094. <https://doi.org/10.3390/s22031094>

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the Regulatory Landscape. *EAI/Springer Innovations in Communication and Computing*, 127–240. <https://doi.org/10.1007/978-3-031-53290-0_3>

Sikder, A. S. (2017). Unveiling the Human Aspect of Cybersecurity: A Holistic Examination of Employee Behavior and Its Significance in Safeguarding Organizational Security within the Context of Bangladesh. *International Journal of Imminent Science & Technology.*, *1*(1), 199–215. <https://doi.org/10.70774/ijist.v1i1.19>

Sikka, V., & Bhayana, P. (2024). Barriers to Comprehensive Financial Inclusion Across the Globe: From Sociocultural Norms to Systemic Challenges. *Sustainable Finance*, 89–126. <https://doi.org/10.1007/978-3-031-67523-2_7>

Stalmachova, K., Chinoracky, R., & Strenitzerova, M. (2022). Changes in business models caused by digital transformation and the COVID-19 pandemic and possibilities of their measurement—case study. *Sustainability*, *14*(1), 127. Mdpi. <https://doi.org/10.3390/su14010127>

Tamplin, T. (2023). *Basel III | Definition, Key Components, Implementation, & Impact*. Finance Strategist. <https://www.financestrategists.com/banking/basel-iii/>

Tamraparani, V. (2025). Leveraging AI for Fraud Detection in Identity and Access Management: A Focus on Large-Scale Customer Data. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.5117225>

Teichmann, F. M., & Boticiu, S. R. (2024). Phishing-Angriffe – Risiken und Herausforderungen für Anwaltskanzleien. *International Cybersecurity Law Review*, *5*. <https://doi.org/10.1365/s43439-024-00110-8>

Val, O. O., Kolade, T. M., Gbadebo, M. O., Selesi-Aina, O., Olateju, O. O., & Olaniyi, O. O. (2024). Strengthening Cybersecurity Measures for the Defense of Critical Infrastructure in the United States. *Asian Journal of Research in Computer Science*, *17*(11), 25–45. <https://doi.org/10.9734/ajrcos/2024/v17i11517>

Vericon. (2024). *2024 Data Breach Investigations Report*. Verizon Business. <https://www.verizon.com/business/resources/reports/dbir/?msockid=2e7b7a8ff19a6b6922d36e50f02e6a07>

Wisista, R. T., & Noveria, A. (2023). Optimizing Pension Fund Investment Portfolio Using Post-modern Portfolio Theory (PMPT) Study Case: An Indonesian Institution. *European Journal of Business and Management Research*, *8*(5), 55–61. <https://doi.org/10.24018/ejbmr.2023.8.5.2097>

Xantrion Cybersecurity. (2024). *Cybersecurity in 2024: Important Insights from Verizon and IBM Reports | Xantrion*. Xantrion. <https://www.xantrion.com/article/cybersecurity-in-2024-important-insights-from-verizon-and-ibm-reports>