International Journal of Accounting and Management Scien
Vol.4 No.4, Oct. 2025
Print ISSN: 2834-8923 Online ISSN: 2832-8175
DOI: https://doi.org/10.56830/IJNZ1133

Global Surge in Banking Frauds: An International Management Perspective

https://www.doi.org/10.56830/IJAMS10202507

Anjali Kale

Michigan State University: East Lansing, Michigan, USA
Email : akale@ennov.com

Sundaranarayanan Viswanathan

Deutsche Post DHL Group: Bonn, North Rhine-Westphalia, DE, USA
Email:Sundaranarayanan.viswanathan@dhl.com

Received: 30 Oct 2025. Accepted: 11 Dec. 2025. Published: 30 Dec. 2025

Abstract

The global banking business has been forced to face an exponential rise in frauds over the last ten years, which was largely because of the speed at which the financial services start becoming digitalized as well as the expansion of cybercriminal networks and the fact that the governance, compliance, and legacy infrastructure remained to be weak. A 2023 report from Aite-Novarica Group further found that fraud-related losses at financial institutions internationally increased by 21 percent between 2018 and 2023, with the report pointing to growth in account takeovers, synthetic identity fraud, and insider collusion many of which could take advantage of the interoperability gaps in legacy systems, splintered cross-jurisdictional regulations (Aite-Novarica Group, 2023). The paper combines the relevance of the academic literature, white papers of the industry, and regulatory guidance to identify the glaring gaps in current strategies namely the lack of exploitation of behavioural analytics and regulatory harmonization across borders. It will have value to new strategies by the senior managers, regulatory bodies, and the design of public policy because of the dynamic threats of frauds in financial systems. Mapping the historical shifts in the face of fraud, check kiting, phishing, and date fabrication through the deep-fake and the mule network and adversarial adversarial dependencies, cross-technological challenges, and geopolitical realities define a framework that the future response might embrace.

Keywords: Banking frauds, financial crime, cybersecurity, international banking, fraud prevention, risk management, top management, compliance

1. Introduction and Background

1.1. Research Problem

The banking institutions have become central to the financial system architecture in the global arena, having towered as the channel of the flow of capital, intermediation of credit, as well as, handlers of risks across jurisdictions. As the financial services are being digitized, fintech platforms emerge, and payment ecosystems become globalized, the inner world of banks has dramatically changed. Although these changes have made customer convenience and improved efficiency possible, they have greatly expanded the area of attack about fraud and financial crime (Accenture, 2023).

The banking industry is currently facing a steep rise in fraudulent activities which are either cyber-driven like malware attacks, phishing and identity theft or oblique such as insider conspiracy, synthetic identities development and foreign nation laundering through trade and shell organisations. Such illegal operations would not only undermine the strength of institutions and customer confidence, but also reveal very serious faults of control of risk management, IT systems, and monitoring and control of regulations (PwC, 2022). The changing character and size of the fraud threat poses a problem to the existing risk management methods and requires a synchronized approach to be adopted by financial institutions, regulators, and international standard-setters.

1.2. Context

The issue of fraudulent banking activity is not a new one and the present forms that it has taken have developed never-before-seen complexity, magnitude and transnational bend. In the past, fraud was especially charged manually where checks were sometimes altered and falsified. Nonetheless, the digital transformation, the expansion of the cross-border flow of capital, and regulatory arbitrage have allowed fraudsters to plan schemes that cross geographical and legal borders (Basel Committee on Banking Supervision, 2021). As an illustrative example, trade finance fraud, an area that has always been considered as low risk because of the use of documentary credit, has become a major source of illicit financial flows. The International Chamber of Commerce (2023) has said they believe trade finance related fraud in 2022 caused losses of over USD 1.5 billion worldwide, and the Singapore and UAE scandals have shown how systems of due diligence and collateral verification are structurally weak at multiple points. In the meantime, both retail and corporate banking customers have faced a serious threat of the spread of account takeover (ATO) fraud.

One specific country called Germany and the UK are major markets in Europe where ATO events grew more than 30 percent between 2021 and 2022 because of sophisticated social engineering methods and the use of vulnerabilities on multiple platforms (Europol, 2023). At the same time decentralized finance (DeFi), cryptocurrency exchanges, and anonymous transaction channels allow opening new blind spots of the international anti-fraud check. Criminals are expanding their use of peer-to-peer crypto markets, privacy coins, and cross-chain bridges when transferring funds and encrypting their illegal proceeds to avoid existing compliance mechanisms channeled through trackable fiat transfer (FATF, 2022). Such a blistering environment highlights the immediate need to develop an effective risk-based approach to fraud prevention that combines regulatory coordination with near real-time monitoring, and real-time adaptive machine learning techniques.

1.3. Objectives

The major purpose behind this study is to carry out a systematic research on the high rate of frauds that has afflicted the banking industry of the world. Compelled by the knowledge that conventional methods of dealing with fraud may be fast becoming ineffective due to the existence of technologically more advanced threats, regulatory disunity, and changing typologies of criminals, the research is motivated. The following paper describes 4 intertwined goals that will contribute to advancing the scholarly knowledge and provide strategic actions pertaining to both practitioners and policymakers. The first, the study aims at examining the major causes of the increase in banking frauds in the world in terms of structural, technological, regulatory, and behavioral aspects. Factors such as the digitization of financial services, the expansion of open banking and API ecosystems, and the widespread use of digital wallets and cryptocurrencies have reshaped the fraud landscape [6,7]. Socio-political factors such as cross-border regulatory arbitrage and under-resourced compliance functions have created fertile ground for fraud to flourish (PwC, 2022).

Second, the paper aims to critically evaluate the limitations of prior research and institutional practices in detecting, reporting, and mitigating banking fraud. Although substantial literature exists on financial crime and risk management, many frameworks remain reactive, fragmented, or overly reliant on rule-based systems, failing to adapt to the dynamic and adaptive strategies employed by modern fraudsters (Ngai, Hu, Wong, Chen, & Sun, 2011); (Ghosh & Reilly, 2020).

Third, the study will propose advanced frameworks for improved fraud mitigation, integrating insights from artificial intelligence, behavioural analytics, and cybersecurity. These frameworks emphasize a shift from rule-based to intelligence-led and real-time fraud detection systems that combine structured and unstructured data, machine learning (ML) models, and risk scoring techniques (Phua, Lee, Smith, & Gayler, 2010); (IBM, 2023). The framework also prioritizes robust governance mechanisms and internal audit alignment to address both internal and external fraud threats.

Finally, this research aims to examine the strategic implications for top management, board governance, and regulatory policy. With fraud increasingly impacting financial stability and institutional reputation, executive leadership must adopt an enterprise-wide risk perspective.

1.4. Significance of the Study

The growing incidence, sophistication, and impact of banking fraud represent a critical threat not only to individual financial institutions but also to the broader global financial ecosystem. This study holds significance on multiple fronts academic, institutional, and policy-driven by systematically examining the evolving nature of fraud, the underlying systemic vulnerabilities, and the urgent need for adaptive, intelligence-driven response mechanisms.

From an academic perspective, this research contributes to the expanding discourse on financial crime, risk management, and digital security by bridging theoretical frameworks with real-world trends. It addresses a notable gap in existing literature, which often treats banking fraud in isolated contexts or focuses narrowly on technological dimensions without accounting for governance, behavioural, and regulatory complexities (Ngai, Hu, Wong, Chen, & Sun, 2011); (Lagazio, Sherif, & Cushman, 2014); (Ngai, Hu, Wong, Chen, & Sun, 2011); (Lagazio, Sherif, & Cushman, 2014). By integrating cross-regional case studies, empirical data, and interdisciplinary insights, this study enriches the scholarly understanding of how fraud evolves across different institutional and geopolitical environments.

Institutionally, the study provides practical guidance for banking executives, compliance officers, internal auditors, and IT risk managers. As financial fraud becomes more elusive and data-driven, institutions must evolve from reactive compliance-based approaches to proactive and predictive risk management models (PwC, 2022); (Deloitte, 2023). This research proposes strategic frameworks that incorporate artificial intelligence, customer behaviour analytics, and enterprise-wide governance reforms to enable timely detection and response.

At the policy level, the study has implications for national and supranational regulators by highlighting the challenges posed by fragmented regulations and the need for enhanced cross-border cooperation. As financial flows become more global and digitized, a harmonized approach to fraud prevention one that aligns supervisory standards, real-time data sharing protocols, and public-private collaboration is critical for ensuring systemic resilience (Basel Committee on Banking Supervision, 2021); (Financial Action Task Force (FATF), 2012).

2. Literature Review

2.1 Previous Research Findings

The proliferation of banking fraud has been a recurring subject in academic and industry-based studies, particularly with the acceleration of digitization in financial services. Some of the prominent reports and empirical studies have repeatedly pointed out that the tendency to abuse technology, with human errors and vulnerabilities of the systems, represents the most prominent factor pushing financial crimes. In an example, the findings of the Global Economic Crime and Fraud Survey (2022) released by PwC showed that almost 46 percent of mounted financial institutions have been hit with fraud cases over the previous two years, with cyber-enabled fraud (like phishing, ransomware, and credential theft) producing a profitable share of the same (PwC, 2022).

Likewise, Deloitte (2021) highlighted the intersection of OT risk and cybersecurity considering the advent of open banking and third-party systems that have become vehicle vectors of fraud. According to the Association of Certified Fraud Examiners (ACFE, 2020), identity theft, ATM skimming, business email compromise, and internal collusion are some of the most frequent types of fraud, the losses of which, are usually caused by deficiencies in the internal controls and the absence of data governance (Deloitte, 2023); (Association of Certified Fraud Examiners (ACFE), 2023). One of the most interesting contributions by the World Bank (2020) indicated that weak compliance regimes correlate with high incidence of fraud and especially the low-income and middle-income countries. The report identified the following indices of vulnerability as lack of developed regulatory infrastructure, inadequate supervisor capacity as well as low use of modern transactional monitoring tools. The presence of opaque corporate structures and informal financial channels in many emerging markets has exacerbated the risk of fraud, money laundering, and terrorism financing (World Bank, 2020).

2.2. Weaknesses in Past Research

Despite the wealth of literature on financial fraud detection and mitigation, several limitations persist. A common criticism is the over-reliance on forensic and technological analyses that isolate fraud as a technical problem rather than a systemic or managerial issue. Many studies focus narrowly on fraud typologies or on the effectiveness of specific detection tools such as decision trees, support vector machines, or anomaly detection systems, often neglecting broader organizational and behavioural drivers.

Insufficient attention has been paid to the strategic role of top management and board oversight in shaping an institution's fraud risk posture. The influence of executive accountability, ethical leadership, and risk governance culture in enabling or constraining fraudulent behavior is under-researched.

2.3 Emerging Perspectives

Recent scholarship and industry reports advocate for a paradigm shift toward interdisciplinary frameworks that blend behavioral finance, artificial intelligence, data science, and international regulatory theory. Researchers have begun to argue that understanding fraud vulnerability requires not only technical tools but also insights into human behavior, incentive structures, and governance failures (Zhao, Xie, & Li, 2021).

One such direction involves applying behavioral analytics and machine learning to detect deviations in transactional behavior in near real-time. These tools go beyond traditional rule-based alerts by learning patterns and identifying anomalies without predefined criteria Simultaneously, there is growing interest in evaluating how corporate culture particularly leadership tone at the top, ethical norms, and employee morale can either deter or exacerbate internal fraud risks (Braun & Clarke, 2006).

From a regulatory standpoint, emerging perspectives stress the importance of harmonized global standards, particularly for digital assets, cross-border payments, and Know-Your-Customer (KYC) obligations. The Financial Action Task Force (FATF, 2022) and the Basel Committee (2021) have called for enhanced cooperation between regulators, banks, fintech firms, and law enforcement to address loopholes created by jurisdictional fragmentation (Basel Committee on Banking Supervision, 2021); (Financial Action Task Force (FATF), 2012).

This study positions itself within this emergent body of research by proposing an integrated, risk-based fraud prevention framework that addresses managerial accountability, technological innovation, behavioural drivers, and international regulatory coherence.

3. Methodology

The research uses qualitative and exploratory research design with an aim of comprehending the multidimensional character of banking fraud within the world jurisdictions. Considering the multifaceted and dynamic nature of mechanisms of fraud, it is not surprising that qualitative methods can help in the investigation of relationships (involving nuances), institutional behaviours, and regulatory issues, not captured by quantitative models (Creswell, 2013); (Yin, 2018)[17,18].

3.1. Research Design and Rationale

The thematic analysis framework makes the study possible because the researcher can identify patterns and insights that have been confirmed through different sources of qualitative data. Triangulating the research findings will be achieved by combining secondary data analysis with semi-structured interviews containing expertise of the major stakeholders, as well as via international comparisons of cases. The approach of methodological research triangulation boosts the credibility and transferability of the findings (Denzin, 2012); (Patton, 2015).

3.2. Data Collection

3.2.1 Secondary Data Sources

Secondary data was drawn from an extensive review of:

- Regulatory publications (e.g., Financial Action Task Force [FATF], Basel Committee on Banking Supervision)
- Industry white papers (e.g., reports by PwC, Deloitte, and McKinsey)
- Peer-reviewed academic journals (e.g., *Journal of Financial Crime*, *Decision Support Systems*)

- Policy briefings from international bodies such as the IMF and World Bank

These sources provided insights into fraud typologies, enforcement strategies, compliance practices, and emerging risks in financial systems.

3.2.2. Expert Interviews

To deepen contextual understanding, semi-structured interviews were conducted with 12 professionals from leading banks and regulatory agencies across APAC, EMEA, and the Americas. Participants were selected based on their roles in:

- Compliance and Anti-Money Laundering (AML)
- Risk Management and Internal Audit
- Cybersecurity and Information Assurance

Interview questions were designed to explore practical challenges, organizational responses to fraud, and views on the effectiveness of existing frameworks. The interviews, conducted via secure video conferencing, were transcribed and thematically coded using NVivo software to identify emerging themes (Braun & Clarke, Using thematic analysis in psychology, 2006).

3.2.3. Case Study Selection

Three international case studies were selected for in-depth analysis, each representing different types of banking fraud and regulatory contexts:

1. Trade-based money laundering in Southeast Asia
2. Synthetic identity fraud in North America
3. Insider collusion and cyber fraud in the EU banking sector

Cases were chosen based on their coverage in regulatory investigations, the availability of reliable documentation, and their relevance to the study's objectives.

3.3. Data Analysis Approach

Data from all sources were analyzed using thematic coding, following Braun and Clarke's (2006) six-phase process: familiarization with data, generation of initial codes, searching for themes, reviewing themes, defining, and naming themes, and producing the report. Themes were organized into categories aligning with the study's analytical lenses: technological, regulatory, managerial, and behavioral.

Thematic findings were then compared across data sets to identify convergent insights and discrepancies, which were interpreted within a broader conceptual framework of fraud risk and governance. This interpretive approach is consistent with qualitative paradigms that prioritize depth, complexity, and contextual meaning (Lincoln & Guba, 1985).

4. Key Findings and Analysis

This section presents the empirical insights derived from thematic analysis of interviews, secondary data, and case studies. It categorizes fraud types, interprets emerging fraud patterns, and evaluates their financial and organizational impacts across the global banking sector.

4.1. Common Types of Banking Fraud

The study confirms the increasing breadth and sophistication of banking frauds, many of which intersect with regulatory weaknesses, rapid digitization, and internal governance failures. The most frequently encountered fraud typologies are as follows:

Account Takeover (ATO)

Account takeover fraud remains among the most prevalent attack vectors, driven by phishing, credential stuffing, and the use of malware to gain unauthorized access to bank accounts. As noted in KPMG's Global Banking Fraud Survey (2022), ATOs have surged by over 30% in North America alone, particularly during the pandemic era, where digital banking became the default mode of transaction (KPMG, 2022).

Synthetic Identity Fraud

This involves creating accounts using a blend of fictitious and real information (e.g., a false name paired with a valid Social Security Number). McKinsey & Company (2021) estimates that synthetic identity fraud now accounts for 10–15% of all credit losses in certain financial institutions, posing a serious detection challenge due to its hybrid nature (Deloitte, 2021); (McKinsey & Company., 2022).

Trade Finance Fraud

Documentary fraud—such as over-invoicing, false bills of lading, and duplicate financing—has grown across emerging markets. According to the International Chamber of Commerce (ICC, 2023), global trade finance fraud led to losses exceeding USD 1.5 billion in 2022, often enabled by cross-border opacity and inadequate verification mechanisms (International Chamber of Commerce (ICC), 2023).

Insider Collusion

Internal fraud involving employee misconduct, collusion with external fraudsters, or manipulation of internal controls continues to threaten institutional integrity. The Association of Certified Fraud Examiners (ACFE, 2022) found that insider involvement contributed to 27% of fraud cases in financial institutions, with average losses significantly higher than external-only frauds (Association of Certified Fraud Examiners (ACFE), 2022).

Payment Fraud

This category encompasses fraudulent ACH transactions, wire transfer manipulation, and point-of-sale system tampering. Real-time payment systems, while efficient, have also become a preferred medium for instant fraud, especially in jurisdictions with underdeveloped fraud detection frameworks (PwC, 2022).

Money Laundering

Criminal enterprises continue to exploit weak AML controls by layering transactions and routing illicit funds through multiple jurisdictions. The Financial Action Task Force (FATF, 2023) reported a marked increase in the use of shell companies and digital currencies in layering and integration stages, especially in trade-based money laundering schemes (Financial Action Task Force (FATF), 2012).

Cyber Frauds

Attacks leveraging ransomware, advanced persistent threats (APT), and zero-day exploits are increasingly targeting financial institutions. IBM's Cost of a Data Breach Report (2023) places the average cost of a banking sector breach at USD 5.9 million, underscoring the gravity of cybersecurity lapses.

Internal Frauds

These have been embezzlement, unauthorized tampering of financial records, and repression of dubious transaction reports. Inadequate supervision, a negative corporate culture, and failures within the audit functions all help sustain the existence of such frauds (Deloitte, 2021).

Regulatory Arbitrage

Lawbreakers take advantage of the dissimilarity in governance especially when it is a cross-nation scenario and each financial framework varies in greater clarity and operation. This loophole was identified by the World Bank (2020) as among the contributors of illicit financial flows (IFFs) especially in tax havens and offshore jurisdictions.

4.2. Impact Analysis

The totalled effect of banking frauds is more than about money conveyed, and it has an impact on the institutional strength, on the faith of customers and on the generality stability of the financial system.

Financial Losses

Financial fraud losses experienced by global financial institutions globally in the year 2023 (and expected to continue to be high in the upcoming years) amounted to more than USD 30 billion in direct loss with each individual case estimating to cost an organization an average of USD 2.4 million (Aite-Novarica Group, 2023). This incorporates operational losses, legal costs, compensation of customer and the cost of recovery of cybersecurity costs.

Reputational Harm

One of the major but rather intangible assets in banking is reputation. An average decrease in the Net Promoter Scores (NPS) after a fraud-related breach was 15 percent in institutions where breaches were reported (McKinsey & Company., 2022). Large fraud disclosures are frequent to be followed by customer defection and investor cynicism.

Operational Burden

The war on fraud is becoming increasingly expensive. Banks are spending millions on hiring more compliance officers, fraud monitoring system, and training. According to reports maintained by the industry, the cost of fraud management has been on the increase at a compound rate of 20 per annum in the last five years (PwC, 2022).

Regulatory Fines

Violations in anti-fraud and AML policies have been followed by very significant fines. As an example several multinational banks were fined over 5% of their turnover in any one year in failure of transaction monitoring, customer due diligence, or suspicious activity reporting (Financial Conduct Authority (FCA), 2023).

Systemic Risk

When the frauds are on a huge scale, they can disturb the global financial systems especially where the central participants like the clearinghouses or the correspondent banks have been involved. The following cross-border frauds that resulted in market distrust and liquidity complaints as was the case in the Wirecard scandal and Danske Bank AML case are threats to contagion as well (European Banking Authority, 2019).

Table 1: High-Profile Fraud cases, Source: [25,29,30]

Fraud Case	Country	Year	Type	Financial Impact (USD)
Wirecard AG	Germany	2020	Financial Statement Fraud	2.1 Billion
PNB Scam	India	2018	SWIFT Misuse	1.8 Billion
Wells Fargo	USA	2016	Unauthorized Accounts	185 Million (fines)
Danske Bank	Denmark	2018	Money Laundering	230 Billion (flow)
Banco Espírito Santo	Portugal	2014	Embezzlement	5 Billion
Allied Irish Bank	Ireland	2002	Rogue Trading	691 Million
Société	France	2008	Rogue Trading	7.2 Billion

Générale				
Standard Chartered	UK	2012	AML Violations	667 Million
JPMorgan Chase	USA	2012	London Whale	6.2 Billion
Olympus Corp	Japan	2011	Accounting Fraud	1.7 Billion

4.3. Driving Factors

The proliferation of banking fraud in the modern financial ecosystem is underpinned by a confluence of technological, regulatory, and organizational vulnerabilities. This section explores the primary systemic drivers contributing to the escalation of fraud in global banking institutions.

4.3.1. Digital Banking Adoption Without Parallel Security Upgrades

The rushed adoption of digital banking services has essentially altered customer interaction and transactions processing. This transition has brought new complex cyber security issues even though it has made it more accessible and efficient in its operations. Numerous financial facilities did not simultaneously modernize their cybersecurity systems after having launched digitalization, which only extended the areas of attacks by the threat actors.

The most up-to-date study on the Cost of Data Breach Report (2023) by IBM confirmed that the second-highest average cost per breach worldwide was in the financial sector, where the breaches cost up to 5.9 million dollars on average, most of which was related to issues with online and mobile platforms (IBM, 2023). Besides, a study conducted by PwC Global Economic Crime and Fraud Survey (2022) revealed the 46 percent of financial institutions have detected digital payment channel-related fraud, indicating the sector is failing to align innovation with cyber resiliency (PwC, 2022).

4.3.2. Increasing Legal Complexity of Cross-Border Operations

Globalization has made it possible to give customers and counterparties the possibility to serve them in other jurisdictions, and therefore has brought a regulatory blind spot. International financial laws are rather atomized, which contributes to discrepancies in the anti-fraud efforts and enforcement capacities. Criminals often abound in these gaps to cover illegal transactions by jurisdiction hopping and sophisticated layering.

Indicatively, the Financial Action Task Force (FATF) has made periodic declarations that the differences in AML/CFT (Anti-Money Laundering/Combating the Financing of Terrorism) enforcement occur between countries, which promotes the laundering of money across geographical boundaries (Financial Action Task Force (FATF), 2012). The example of Wirecard that covered more than 20 countries shows how the lack of regulatory coordination allowed the company to cover up frauds as it was supervised by several national regulators (European Parliament, 2021).

4.3.3. Legacy Systems Lacking Advanced Protections

Even though technology has shaken the world by evolving at a rapid rate, numerous banks still have their core banking infrastructure which is old fashioned with not sufficient security and interoperate with the newer systems to detect the newer frauds. Legacy platforms tend to lack the capability to support real-time monitoring and behavioral analytics or anomaly detection by machine learning, which exposes the system to internal and external threats on a systemic level. According to the World Bank (2020), half of the questioned banks in low- and middle-income economies used legacy systems, which were prone to fraud, especially in trade finance and interbank transfers (World Bank, 2020) The old systems also make it harder to adopt new, high-security protocols and incorporate cybersecurity updates, which helps to continue maintaining structural insecurity.

4.3.4. Gaps in Internal Controls and Oversight

Internal fraud and collusion are also endangering factors, especially when there is inefficient governing mechanism, compliance monitoring and ethical control in an institution. The proposed policy that can be observed under the high-profile incidents, as in the case of the Punjab National Bank (PNB) fraud in India when insiders invoked fraudulent Letters of Undertaking through the SWIFT network, demonstrates how the failure of internal controls may lead to astronomical losses. According to the post incident review by Reserve Bank of India (RBI) the fraud might have been averted by adherence to more stringent reconciliation of SWIFT and core banking systems (Reserve Bank of India, 2018).

4.4. Challenges for Top Management

In the face of escalating fraud threats, senior management in banking institutions confronts a complex array of strategic, operational, and reputational challenges. These challenges are not merely technological but deeply embedded in governance frameworks, risk cultures, and leadership accountability. As fraud tactics evolve in sophistication, so too must the leadership's capacity to anticipate, mitigate, and respond to such risks effectively.

4.4.1. Aligning Innovation with Cybersecurity

The banking sector has aggressively pursued digital innovation to meet evolving customer expectations and remain competitive, often by adopting mobile banking platforms, open banking APIs, and AI-driven financial services. However, this rapid digitization frequently lacks a parallel investment in robust cybersecurity controls. Research by (Capgemini, 2022) found that while 80% of banks accelerated digital transformation efforts post-COVID-19, only 21% reported cybersecurity as a key strategic priority during those implementations (Capgemini, 2022). This misalignment exposes institutions to vulnerabilities such as API breaches, ransomware attacks, and identity fraud. Top management must ensure that innovation strategies are not siloed from cybersecurity planning but embedded in a “security-by-design” approach, with chief information security officers (CISOs) and risk leader’s integral to the product development lifecycle.

4.4.2. Coordinating Multinational Fraud Response

Financial institutions operating across borders face heightened difficulty in responding to fraud due to divergent legal regimes, regulatory expectations, and enforcement capabilities. Cross-jurisdictional fraud cases require centralized visibility into incidents and a coordinated strategy for legal compliance, investigation, and remediation. For instance, the Wirecard scandal exposed weaknesses in regulatory oversight, where national regulators failed to share intelligence effectively or respond with unified urgency despite red flags being raised in multiple countries (European Parliament, 2021). In a survey conducted by Deloitte (2021), 57% of global banking executives cited regulatory fragmentation as a key barrier to timely fraud response (Deloitte, 2021). Leadership must develop cross-border collaboration frameworks that allow real-time threat intelligence sharing, joint compliance task forces, and agile response mechanisms that account for local legal nuances.

4.4.3. Managing Reputational Fallout and Legal Risks

Fraud incidents not only incur financial losses but also pose existential risks to a bank’s brand reputation, investor confidence, and regulatory standing. According to Accenture (2023), nearly 72% of customers are less likely to continue banking with an institution that suffers a major fraud incident, even if their accounts are unaffected (Accenture, 2023). Furthermore, regulators have adopted a more punitive stance, imposing multi-million-dollar fines for failures in fraud detection, governance oversight, or AML compliance.

An example is of Goldman Sachs, which has been fined $2.9 billion in 2020 because of its role in the 1MDB scandal, and another one is of Danske Bank that has been slapped with penalties of 2 billion in 2022 in relation to its AML failure entailing its Estonian branch. Such incidences reflect the increase of legal risks associated with executive negligence or failure to supervise. Therefore, the top management should institutionalize governance of fraud risk in the board room, establish crisis communication practices, as well as perform regular stress testing exercises, based on scenarios. The stewardship by the top management, portrayed by transparent disclosure, ethical leadership, and proactive compliance, plays an important role in ensuring trust and resilience of the institution following fraud events.

4.5. Case Examples

Case studies can be regarded as an excellent contribution to the practice of what fraud risks can be in terms of systemic weakenesses of worldwide bank operations. In the case provided, Wirecard, Punjab National Bank (PNB), and Wells Fargo, the instances support the idea that fraud can occur in enterprise dimensions and is facilitated by governance failure, existence of loopholes in technology, and the cancerous organizational culture. These instances serve as the present urgency of coherent internal regulatory systems, strength of internal control and ethical leadership.

4.5.1. Wirecard: Exposed Regulatory Gaps and Weak Governance

The recent corporate fraud of the Wirecard AG in 2020 can be globally seen and called as one of the major in the European corporate history. Although a regulated institution whose stock was listed in the DAX index of Germany, Wirecard succeeded in faking balance sheets by exaggerating the assets and increasing revenues by means of non-existing third party acquirers in Asia.

More than 1.9 billion euro of alleged bank balances were realized to be false. The scandal revealed serious gaps in both internal governance and some of its after-the-fact regulation, such as the inability of Germany financial regulator, BaFin, to act with decisiveness in response to whistleblower complaints and red flags about flagitious activity raised by external journalists and short sellers (European Parliament, 2021). The case demonstrated the extreme dependence on external auditors and the necessity to restructure the cross-border regulatory cooperation, transparency and enforcement across the EU.

4.5.2. Punjab National Bank (PNB) Scam: Insider Misuse of the SWIFT Network

One of the largest banking frauds on Indian history occurred in 2018; the PNB fraud, with the amount of about 13,000 crore (USD 1.8 billion). The case involved a set of employees who used the SWIFT (Society of Worldwide Interbank Financial Telecommunication) system to issue unauthorised Letters of Undertaking (LoUs) to overseas branches of Indian banks. These LoUs did not reflect on the core banking system of the bank and this helped the perpetrators to skip around internal checks and audit (Reserve Bank of India, 2018). The case illustrated a grave gap between real-time risk control systems and operations of SWIFT. Further, it brought up sore questions as to the ethical standards, protection given to the whistleblowers and strongness of supervisory control in the Government banks. Following it, the Reserve Bank of India required that SWIFT and core banking systems be much more tightly integrated and that there be real time reconciliation and audit trails in its aftermath.

Wells Fargo: Ethical Lapses and Cultural Issues

The case of fake accounts at Wells Fargo which surfaced in 2016, presents an example of how unhealthy corporate culture, and distorted incentive systems can lead to pervasive fraud. Workers under pressure to achieve high sales of cross-selling entered more than 3.5 million unethical bank accounts and credit card accounts in the names of their customers without their consent. Although the financial losses were immense (more than 3 billion dollars in regulatory fines and settlements) the loss in reputation and damage to the stakeholder trust was much greater (U.S. House Financial Services Committee, 2020). It was found that the highest executives had long been disregarding the internal alerts and developed the atmosphere of fear in which any reporting of unscrupulous behavior could lead to persecution. The case has now been used to illustrate a warning in corporate governance and has allowed regulatory changes in the following areas of accountability, aligning incentives and reflecting responsibility of risk culture at board level.

4.6. Regulatory and Industry Measures

The high rise in banking fraud across the world has required a dimensional approach by regulators and industry organizations. Different legislative, regulatory, and technological solutions have been proposed in jurisdictions in a bid to enhance the strength of financial systems. These initiatives are focusing on risk-based compliance, cybersecurity, protection of customers and data confidentiality. Nevertheless, there is still a gap in enforcement and implementation, especially where international borders are concerned. In this segment, the author reviews some major regulatory and industry-led initiatives that can be used to reduce financial crime and improve institutional oversight.

4.6.1. PSD2 and SCA: Multi-Factor Authentication in the EU

In March 2018, the European Union introduced the Revised Payment Services Directive (PSD2) that represented the paradigm shift in the regulation of digital payments with the establishment of such principle as Strong Customer Authentication (SCA). SCA includes multifactor in the sense of authentication that requires two or more factors from knowledge (e.g., password), possession (e.g., mobile device) and inherence (e.g., biometrics) categories, thus fractionating fraud during electronic transactions to a massive extent [33]. The PSD2 also recognizes the secured competitive innovation in open banking by terms of compelling financial institutions together with other third-party payment providers to improve their authentication procedures. There has been however noted implementation difficulties especially among the smaller banks and merchants who were facing implementation difficulties due to their technical requirements of the integrating compliance issues and requirements.

4.6.2. FATF: Emphasis on Risk-Based AML Practices

An intergovernmental organization, the Financial Action Task Force (FATF), is the central organization that determines international policies in the field of Anti-Money Laundering (AML) and combating terrorist financing (CFT). In the 2012 Recommendations, Mr. FATF advocates a risk-based approach that encourages financial organizations to adapt due diligence, monitoring and reporting to the level of risk that the customer presents, the complexity of the products to offer and geographic exposure (Financial Action Task Force (FATF), 2012). The method is more cost effective and increases the probability of catching fraud since the low risk clients will not be subjected to over-sight. FATF under leadership has not succeeded in ensuring uniform implementation especially to developing economies that have little infrastructure of compliance.

4.6.3. SWIFT Customer Security Programme (CSP): Standards for Cyber Resilience

In response to a series of high-profile fraud incidents, including the 2016 Bangladesh Bank cyber heist, the SWIFT Customer Security Programme (CSP) was introduced to improve the security posture of financial institutions using the SWIFT network. CSP establishes baseline controls covering secure network access, malware protection, and incident response. As of 2023, compliance with the CSP's 25 mandatory and advisory controls is required annually, subject to external validation (SWIFT, 2023). CSP has enhanced institutional readiness, though studies suggest that real-time detection and coordinated information sharing remain limited across jurisdictions.

4.6.4. USA PATRIOT Act and BSA: Enhanced KYC and Reporting

The USA PATRIOT Act (2001) and the Bank Secrecy Act (BSA) (1970) form the backbone of the United States' AML framework. Under these laws, financial institutions have been required to put in place effective Know Your Customer (KYC) measures, keep a record of cash transactions, and file Suspicious Activity Reports (SARs) of suspicious activity. Title III of PATRIOT Act considerably expanded the AML regime by increasing the due diligence standards of foreign correspondent accounts and integrating information-sharing capabilities with other institutions (FinCEN, 2021). These measures have brought about increased transparency as well as creating compliance costs, especially to the community banks and the fintech startups.

Data Privacy Laws: GDPR and CCPA Enforcement

The emergence of fraud detection applications has increased the conflict between data privacy and fraud prevention leading to the development of stringent data governance policies by the regulators. Such efforts include the General Data Protection Regulation (GDPR), the legislation by the European Union and the Consumer Privacy Act (CCPA), the California one. The two frameworks allow individuals to have power over their personal data and set tight restrictions on the usage, collection, and storage of personal data even in terms of fraud purposes (European Commission, 2019); (State of California, 2020). The financial institutions now have to toe the line between efficient fraud surveillance and the demands of compliance regarding user requirement, limitation of data and breach reporting.

4.7. Technological Defences

Technology is therefore crucial in strengthing institutional defence as the dexterity and the zest of banking fraud keeps on increasing with multifaceted and multiplied magnitude. Although regulatory frameworks provide structure, resilience against emerging threats can only be achieved through advanced technological interventions via real time detection and prevention of the threat. With a combination of machine learning (ML), biometric profiling, distributed ledger technologies and artificial intelligence (AI), the financial sector is once again transforming on how to spot unusual behavior, identify users and investigate networks with suspicion. This part looks at sophisticated tools and how best they can be used in fighting modern fraud in banks.

4.7.1. Artificial Intelligence and Machine Learning: Real-Time Anomaly Detection

AI and ML systems are increasingly deployed to analyze high-frequency, high-volume transaction data in real-time, identifying deviations from normative behavior that may signal fraud. Supervised learning models trained on historical fraud datasets can flag recurring patterns, while unsupervised algorithms can detect new or unknown fraud typologies by clustering irregularities (Nasir, Arshad, & Ahmad, 2021). JPMorgan Chase, for example, has implemented ML-based risk scoring mechanisms that evaluate transactions across millions of accounts in seconds, significantly reducing false positives and response time (JPMorgan Annual Report, 2022). However, concerns around explainability, model bias, and data quality continue to affect widespread adoption.

4.7.2. Behavioural Biometrics: Typing Patterns and Device Behaviour

Behavioral biometrics, which analyze user-specific interaction patterns such as keystroke dynamics, touchscreen pressure, mouse movements, and device orientation, offer a passive and continuous form of authentication. Unlike static credentials, these identifiers are difficult for fraudsters to replicate, especially during account takeover attempts. Financial institutions like HSBC and Barclays have integrated behavioral analytics to detect imposters even after login credentials are compromised (Khan, Farooq, & Ikram, 2022). These systems operate silently in the background, enhancing security without degrading user experience. Yet, data privacy regulations such as GDPR require institutions to ensure transparent and consensual usage.

4.7.3. Graph Analytics: Mapping Fraud Networks

Graph analytics employs interconnected data models to uncover hidden relationships between seemingly disparate transactions, accounts, or entities. This is particularly effective in identifying collusive fraud, mule accounts, or layered money laundering structures that evade traditional rule-based systems. By visualizing transactional linkages, institutions can trace suspicious nodes and paths, allowing for preemptive action. A study by IBM (2020) demonstrated how graph-based models improved fraud detection accuracy by over 30% when applied to transactional datasets in Southeast Asia. These tools are also being deployed by regulators for systemic surveillance (Sharma & Shukla, 2023).

4.7.4. Blockchain: Transparent Trade Finance Records

Blockchain technology introduces an immutable and decentralized ledger that significantly reduces the risk of document tampering, duplicate invoicing, and identity spoofing—common in trade finance fraud. Projects such as Marco Polo and Contour leverage blockchain to digitize letters of credit and bills of lading, creating shared visibility among importers, exporters, banks, and regulators (European Parliament, 2021). The traceability and consensus mechanisms inherent in blockchain systems enhance auditability, while smart contracts automate compliance checks. Nevertheless, interoperability and regulatory uncertainty continue to hinder mainstream adoption.

Table 2: Technology Solutions Pros and Cons

Solution	Pros	Cons
AI Monitoring	Real-time insights	Complex model governance
Biometrics	Seamless security	Privacy risks
Blockchain	Immutable records	Limited adoption
Graph Analytics	Network insights	Data dependency
Adaptive MFA	Contextual control	High setup cost

5. Discussion and Interpretation

The findings of this study reveal that fraud in the global banking sector is not merely a technological or operational issue but a multi-dimensional challenge requiring strategic leadership, robust governance, and global regulatory alignment. This section synthesizes the implications for banking executives and explores practical and organizational barriers that may impede effective implementation of anti-fraud frameworks.

5.1 Implications for Executives

Banking executives are uniquely positioned to shape institutional resilience against fraud. Beyond compliance enforcement, leadership must actively cultivate a culture of integrity and risk awareness throughout the organization. Tone at the top—an established principle in governance literature has been repeatedly linked to lower incidences of internal fraud and misconduct (PwC, 2022). Executives must champion investments in advanced analytics, such as AI-driven risk scoring and behavioural biometrics, while ensuring cross-functional integration across compliance, IT, legal, and audit units.

Furthermore, senior management plays a pivotal role in aligning business innovation with cybersecurity imperatives. For example, as banks adopt open banking and decentralized finance (DeFi) platforms, executive leadership must oversee adaptive risk models and ensure that digital transformation does not outpace controls (Deloitte, 2023). Active board oversight, coupled with strategic partnerships with fintech and regtech players, can strengthen the bank's fraud detection capacity without compromising agility.

5.2. Implementation Challenges

Despite promising technological advances and regulatory reforms, several challenges impede the effective execution of anti-fraud strategies:

5.2.1. High False Positives from Sensitive Models

AI and ML-based detection systems, while powerful, often produce high false positive rates, overwhelming compliance teams and delaying legitimate transactions. Studies estimate that nearly 90–95% of flagged alerts in traditional rule-based anti-money laundering (AML) systems are false positives (McKinsey & Company., 2022). Fine-tuning models without compromising sensitivity remains a pressing challenge.

5.2.2. Data Silos Between Banking Systems

Many banks operate within fragmented IT ecosystems where customer data, transactional records, and fraud indicators reside in disconnected databases. These silos hinder real-time surveillance and cross-functional insights. Integrated data lakes and secure API-based architectures are required to unify fraud intelligence and support end-to-end monitoring (Accenture, 2023).

5.2.3. Shortage of Specialized Fraud Professionals

The talent gap in fraud analytics, cybersecurity, and forensic accounting has widened in recent years. As financial crimes become more technically sophisticated, banks struggle to hire and retain professionals who possess interdisciplinary expertise in AI, compliance, and behavioral risk management (Europol, 2023). Upskilling and internal capability development are therefore critical to sustaining defense operations.

5.2.4. AI Governance Complexities

While AI tools enhance fraud detection, their use raises ethical and operational concerns around explainability, accountability, and regulatory compliance. Institutions must develop internal governance mechanisms to monitor model drift, ensure fairness, and comply with evolving AI-related laws such as the EU's AI Act (OECD, 2021).

5.2.5. Limited Cross-Border Cooperation

Fraud networks often exploit jurisdictional boundaries, operating across countries with divergent legal and regulatory standards. The lack of harmonized frameworks, data-sharing protocols, and investigative collaboration limits the global fight against financial crime. Initiatives like the Egmont Group and the Financial Action Task Force (FATF) have made progress, but operational coordination among national financial intelligence units (FIUs) remains inconsistent (Financial Action Task Force (FATF), 2012).

5.3 Strategic Opportunities

5.3.1. AI and ML for Predictive Detection

Artificial intelligence (AI) and machine learning (ML) present significant opportunities to move beyond rule-based fraud detection systems toward predictive and adaptive solutions. These technologies can process vast volumes of transactional data in real-time, identify anomalous behavior patterns, and flag suspicious activities with far greater accuracy than traditional methods. Predictive ML models can learn from historical fraud data, enabling dynamic risk scoring and behavior-based authentication (Deloitte, 2021);. (Bai, Chai, & Raza, 2021) When embedded within core banking workflows, such systems can also enhance early warning mechanisms and reduce the window for fraud execution.

5.3.2. Blockchain for Transparency

Blockchain technology offers significant promise in improving transactional transparency and immutability, particularly in areas like trade finance and cross-border payments. Distributed ledger systems can reduce fraud risks by creating tamper-proof audit trails, automating verification via smart contracts, and minimizing opportunities for document forgery (PwC, 2022); (World Economic Forum, 2020). In trade finance, for instance, blockchain-enabled platforms can eliminate duplication of invoices, false shipping documents, and manipulation of letters of credit, all of which have been instrumental in large-scale frauds.

5.3.3. Shared Threat Intelligence Networks

Another strategic opportunity lies in the formation of shared threat intelligence ecosystems. Banks, regulators, and cybersecurity firms can collaborate through secure platforms to exchange information on emerging fraud typologies, attack vectors, and threat actor profiles. Initiatives such as the Financial Services Information Sharing and Analysis Center (FS-ISAC) exemplify the benefits of collective defense through coordinated incident response and real-time alerts (FS-ISAC, 2023). Establishing regional and global consortia to facilitate trusted data exchange can greatly enhance situational awareness and resilience, especially against cross-border cybercriminal syndicates.

5.4 Risks and Limitations

Despite the promise of emerging technologies and cross-sector partnerships, certain systemic risks and practical constraints must be carefully considered in designing effective fraud mitigation strategies.

5.4.1. Overdependence on Automation

While AI and automation improve operational efficiency, overreliance on these technologies without adequate human oversight can be dangerous. AI systems may generate false positives, overlook novel fraud schemes, or fail to adapt to rapidly changing behavioral patterns without continuous retraining. In critical situations, automation without escalation paths to human analysts may delay appropriate responses (Microsoft, 2021). Moreover, financial institutions risk “model complacency,” wherein the perception of technological superiority diminishes the vigilance of risk managers.

5.4.2. Ethical Concerns on Surveillance

Such technologies as behavioural biometrics, deep packet inspection, and transaction profiling are technically raising severe ethical and privacy issues. Yet, despite helping to detect frauds, such tools also infringe on the border between surveillance and security and thus restrict individual rights and data protection act like the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the U.S. (State of California, 2020). The practices of AI ethics require fraud detection systems to include fairness, transparency, and accountability of algorithm decisions.

5.4.3. Regulatory Fragmentation Across Regions

An unequal regulatory establishment internationally is one of the outstanding impediments to a unified fight in countering fraud. The global banks must deal with incongruent compliance requirements, information-sharing limitations, and regulatory anticipations. Although international frameworks, such as FATF, to some extent offer background information, different national regulators apply and enact these standards and end up creating gaps and inconsistencies in their application (Basel Committee on Banking Supervision, 2021); (Financial Action Task Force (FATF), 2012). These disparities are particularly pronounced in anti-money laundering (AML) and cybersecurity laws, hindering global cooperation and creating safe havens for fraudsters.

5.5 Future Research Directions

The dynamic and evolving nature of banking fraud necessitates continued scholarly inquiry and innovation. While significant advancements have been made in understanding fraud typologies and deploying technological countermeasures, several underexplored dimensions offer fruitful opportunities for future research. These include cross-cultural response mechanisms, the effectiveness of internal whistleblower systems, and the development of standardized global risk indices.

5.5.1. Comparative Studies on Fraud Response Across Cultures

Future studies should explore how cultural dimensions influence fraud detection, prevention, and institutional responses. Hofstede's cultural dimensions theory underscores how national culture affects ethical behavior, risk perception, and organizational controls (Hofstede, 2011). For example, high power distance cultures may discourage junior staff from reporting irregularities, while collectivist cultures may prioritize group loyalty over regulatory compliance. Comparative research across regions such as North America, the Middle East, and

East Asia can reveal variations in fraud reporting behavior, regulatory enforcement, and ethical norms, offering insights into tailored fraud mitigation strategies (Kassem & Higson, 2016). Integrating cultural intelligence into compliance frameworks could thus enhance their global applicability and effectiveness.

5.5.2. Evaluation of Whistleblower Frameworks Globally

Whistleblower protection is a critical, yet inconsistently implemented, component of institutional fraud resilience. While laws like the U.S. Dodd-Frank Act and the EU Whistleblower Protection Directive offer substantial legal safeguards, many jurisdictions still lack robust legal frameworks or cultural support for internal disclosures (European Commission, 2019); (OECD, 2021). Future empirical research should assess the implementation, uptake, and outcomes of whistleblower programs across different legal and corporate contexts. Key variables include anonymity guarantees, organizational retaliation, financial incentives, and impact on fraud detection rates. Such research could inform best practices for establishing transparent, psychologically safe mechanisms for internal fraud reporting.

5.5.3. Creation of Global Fraud Risk Indices

There is currently no standardized, cross-jurisdictional index to quantify banking fraud risk in a globally comparable manner. Existing indices, such as Transparency International's Corruption Perceptions Index or the Basel AML Index, offer partial proxies but fail to capture sector-specific risks and technological vectors unique to banking fraud. Future research could explore the construction of a comprehensive Global Banking Fraud Risk Index (GBFRI) that synthesizes regulatory data, incident reports, technological maturity, and institutional governance scores. Such an index could aid international financial institutions, investors, and regulators in benchmarking risk exposure and prioritizing resources across regions (Transparency International, 2023).

6. Conclusion

The accelerating frequency and complexity of banking frauds on a global scale highlight the urgent need for a transformative approach to financial governance, technological infrastructure, and executive leadership. This study has demonstrated that the interplay between digitization, cross-border regulatory fragmentation, and evolving criminal tactics has expanded the threat landscape far beyond the capacities of traditional fraud detection mechanisms. In this context, banking institutions can no longer afford to operate within reactive frameworks. Instead, a paradigm shift toward anticipatory and intelligence-driven fraud management is imperative.

The proposed multi-dimensional framework integrates governance reforms, advanced analytics, and human capital development to create a holistic response strategy. It acknowledges that no single measure technological or regulatory is sufficient on its own. As such, institutions must harmonize AI-enhanced surveillance tools, such as real-time anomaly detection systems, with behavioural biometrics and risk-based multi-factor authentication to fortify digital banking interfaces (Braun & Clarke, Using thematic analysis in psychology, 2006); (Lincoln & Guba, 1985). Equally vital is the deployment of distributed ledger technologies (DLT), such as blockchain, particularly in trade finance and cross-border transactions, to ensure transparency and tamper-proof audit trails.

From a policy and governance standpoint, collaborative efforts across jurisdictions are essential. Fragmented regulatory regimes and inconsistent enforcement practices remain significant enablers of financial crime. Thus, enhanced cooperation between central banks, international regulators (e.g., FATF, BIS), and private financial institutions can facilitate unified risk indices, global reporting standards, and real-time threat intelligence networks (Financial Action Task Force (FATF), 2012); (OECD, 2021). Moreover, leadership must foster a risk-aware culture that empowers internal whistleblowers, strengthens ethical norms, and aligns innovation with security mandates.

Ultimately, banking fraud is not merely a technological or operational problem; it is a systemic challenge that reflects the evolving vulnerabilities of a digitized and interconnected financial ecosystem. By adopting a strategic, integrated, and cross-disciplinary approach, financial institutions can mitigate monetary losses, preserve stakeholder confidence, and reinforce the integrity of global financial systems in the digital age.

References:

Accenture. (2023). *Fraud risk management: Redefining the future of trust in banking.* https://www.accenture.com/us-en/insights/banking/fraud-risk-management.

Aite-Novarica Group. (2023). *Global fraud trends: An analysis of financial crime from 2018–2023.* https://aite-novarica.com.

Association of Certified Fraud Examiners (ACFE). (2022). *Report to the Nations on Occupational Fraud and Abuse.* https://www.acfe.com.

Association of Certified Fraud Examiners (ACFE). (2023). Occupational fraud 2022. *A report to the nations*, https://www.acfe.com/report-to-the-nations/2022/.

Bai, X., Chai, X., & Raza, S. A. (2021). Machine learning-based fraud detection in the banking sector. *Journal of Financial Security*, 6(2), 88–102. https://doi.org/10.1016/j.jfs.2021.100882.

Basel Committee on Banking Supervision. (2021). Sound management of risks related to money laundering and financing of terrorism. *Bank for International Settlements*, https://www.bis.org.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77–101. https://doi.org/10.1191/1478088706qp063oa.

Capgemini. (2022). *World retail banking report 2022.*

Capgemini. (2022). *World retail banking report 2022.* https://www.capgemini.com/research/world-retail-banking-report-2022/.

Creswell, J. W. (2013). Qualitative inquiry and research design. *Choosing among five approaches (3rd ed.)*, SAGE Publications.

Deloitte. (2021). *Global financial services regulatory outlook.* https://www2.deloitte.com.

Deloitte. (2023). *AI in fraud detection: Navigating risk with innovation.* https://www2.deloitte.com.

Denzin, N. K. (2012). The research act. *A theoretical introduction to sociological methods*, Aldine Transaction.

European Banking Authority. (2019). *Opinion on the elements of Strong Customer Authentication under PSD2.* https://www.eba.europa.eu.

European Commission. (2019). *Whistleblower Protection Directive (Directive (EU) 2019/1937).* https://eur-lex.europa.eu.

European Parliament. (2021). *Lessons from the Wirecard scandal.* https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)690595.

Europol. (2023). *Internet Organised Crime Threat Assessment (IOCTA).* https://www.europol.europa.eu.

Financial Action Task Force (FATF). (2012). *The FATF recommendations: International standards on combating money laundering and the financing of terrorism & proliferation.* https://www.fatf-gafi.org.

Financial Conduct Authority (FCA). (2023). *Annual enforcement report.* https://www.fca.org.uk.

FinCEN. (2021). *USA PATRIOT Act overview.* https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act.

FS-ISAC. (2023). *Annual report.* https://www.fsisac.com/.

Ghosh, S., & Reilly, D. L. (2020). Credit card fraud detection with a neural-network. *In Proceedings of the 27th International Conference on Neural Information Processing Systems*, (pp. 1–9).

Hofstede, G. (2011). Dimensionalizing cultures: The Hofstede model in context. *Online Readings in Psychology and Culture*, 2(1), 8. https://doi.org/10.9707/2307-0919.1014.

IBM. (2023). *AI-powered fraud detection: A new frontier in banking security.* https://www.ibm.com.

International Chamber of Commerce (ICC). (2023). *Global trade finance survey.* https://iccwbo.org.

Kassem, R., & Higson, A. (2016). The new fraud triangle model. *Journal of Emerging Trends in Economics and Management Sciences*, 7(4), 231–238.

Khan, M. T., Farooq, M. U., & Ikram, N. (2022). Behavioral biometrics for secure authentication: A comprehensive survey. *Computers & Security*, 116, 102903. https://doi.org/10.1016/j.cose.2022.102903.

KPMG. (2022). Global banking fraud survey. *Navigating the evolving threat landscape*, https://home.kpmg.

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, 45, 58–74.

Lincoln, Y. S., & Guba, E. G. (1985). *Naturalistic inquiry.* SAGE Publications.

McKinsey & Company. (2022). Reputation in banking. *How to manage what matters*, https://www.mckinsey.com.

Microsoft. (2021). *The risk of overreliance on automated fraud detection.* https://www.microsoft.com/security/blog.

Nasir, M. U., Arshad, S. Z., & Ahmad, S. (2021). Machine learning-based financial fraud detection: A comparative analysis. *Expert Systems with Applications*, 168, 114122. https://doi.org/10.1016/j.eswa.2020.114122.

Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems*, 50(3), 559–569. https://doi.org/10.1016/j.dss.2010.08.006.

OECD. (2021). *Committing to effective whistleblower protection.* https://www.oecd.org/gov/whistleblower-protection.htm.

Patton, M. Q. (2015). *Qualitative research & evaluation methods (4th ed.).* SAGE Publications.

Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *arXiv preprint arXiv*, 1009.6119.

PwC. (2022). *Global economic crime and fraud survey.* https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html.

Reserve Bank of India. (2018). *Speech on banking frauds and governance.* https://www.rbi.org.in/Scripts/BS_SpeechesView.aspx?Id=1056.

Sharma, R., & Shukla, N. (2023). Network-based detection of financial fraud using graph analytics. *International Journal of Information Management*, 63, 102619. https://doi.org/10.1016/j.ijinfomgt.2022.102619.

State of California. (2020). *California Consumer Privacy Act (CCPA).* https://oag.ca.gov/privacy/ccpa.

SWIFT. (2023). *Customer Security Programme (CSP).* https://www.swift.com/myswift/customer-security-programme-csp.

Transparency International. (2023). *Corruption perceptions index 2023.* https://www.transparency.org/en/cpi.

U.S. House Financial Services Committee. (2020). *Holding Wells Fargo accountable: Examining the role of the board of directors in the bank's egregious pattern of consumer abuses.* https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=406328.

World Bank. (2020). *Digital financial services and the role of legacy banking infrastructure.* https://openknowledge.worldbank.org/handle/10986/34991.

World Bank. (2020). *Illicit financial flows and regulatory responses in global banking.* https://www.worldbank.org.

World Economic Forum. (2020). *The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services.* https://www.weforum.org/whitepapers.

Yin, R. K. (2018). Case study research and applications. *Design and methods (6th ed.)*, SAGE Publications.

Zhao, H., Xie, M., & Li, Y. (2021). Cross-platform banking fraud detection using hybrid deep learning models. *Journal of Financial Crime*, 28(4), 1054–1072.