World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI

Cross Ref DOI: 10.30574/wjarr

Journal homepage: https://wjarr.com/

(Review Article)

The trifecta against financial crime: A collaborative analysis of the roles of banks, consulting firms, and governments

Prince Iheonunekwu *

Independent Researcher, Boston, Massachusetts, USA.

World Journal of Advanced Research and Reviews, 2024, 23(03), 1445–1468

Publication history: Received on 29 July 2024; revised on 06 September 2024; accepted on 09 September 2024

Article DOI: https://doi.org/10.30574/wjarr.2024.23.3.2739

Abstract

The roles of banks, consulting firms and governments are intertwined in combating financial crime. Banks are on the frontlines as they process financial transactions and engage directly with customers. Banks are extraordinarily strategic because they interface with customers and are heavily involved in handling financial transactions worldwide. They watch accounts for any suspicious activity and report such activities to the legal bodies as expected under AML regulations. Consulting firms help banks, as well as other financial organizations to create various tools for evaluating threats and devising strategies for firms to conform to. They also do training in the area of financial crime prevention. Governments put in place measures in the form of legislation that seeks to prevent and curtail acts such as money laundering, financing of terrorism and tax evasion among others.

Materials and Methods: The study's literature was obtained from electronic databases. Only the articles that investigated the effectiveness and efficiency of anti-money laundering/counter-terrorist financing policies and regulations and/or sources that compared financial institutions' cooperation with consulting companies and governmental agencies were included. Among the reviewed sources 53 from 1980 till 2023, which included academic books, journal articles, government and international organization reports.

Results: The literature shows that relying on the regulation is inadequate for controlling finance related crimes. Banks have a profit-driven culture and it lacks scrupulousness towards integrity risks. For the same purpose, prescriptive regulations increase disproportionate compliance costs for small jurisdictions and financial institutions. Companies seeking risk management services get these from consulting firms that also profit from molding compliance frameworks. Syndication enables the employment of unique features possessed by each party. While the banks have an effective network and reach, the consulting firms can analyze data accurately, and the government has statutory power and control.

Discussion: Shifting social norms are another driver: peoples' behavior in financial markets today is a shift from that of even a decade ago and there is a need to address financial crime in a shared manner and increase cooperation at a global level. To put measures in place, the roles and responsibilities should be well defined based on strengths of each of the entities. Banks are also in good shape for transaction monitoring although they need some regulation to do so. Analyzing the motives for consulting firms, it is possible to state that the provision of technical solutions is possible only if there are factors that guarantee the transparency of actions. Governments provided the blueprint in achieving the proportionate, risk adjusted policies while leaving it to the private sector to drive the processes. This is because we have seen that financial globalization means that nations have to ideally move in synchrony. International agencies such as the UN, FATF, FSB, IMF and others have contributed to the development of international standards, whereas in national situations, the effects vary from one country to another.

* Corresponding author: Prince Iheonunekwu

Conclusion: It can therefore be seen that no single entity can deal with such complicated concepts of transnational financial crimes in isolation. The utilization of the mandated strategies by banks, consulting companies and governments as essential collaborators in tandem with their core competencies is the most useful approach. This triumvirate, therefore, has great potential to add real value to anti-financial crime efficiency when properly aligned and adequately supervised in a manner consistently and holistically operationalized.

Keywords: Financial crime; Digital finance; Money laundering; Anti-money laundering (AML); Fintech; Blockchain; Artificial Intelligence (AI); Machine learning; Know Your Customer (KYC); Financial Action Task Force (FATF)

1. Introduction

The appearance of such a concept as digital finance backed by large technology platforms called BigFintechs (BFTs) played a significant role in restructuring the financial environment (Arner et al., 2021). At the same time, barred easy access to essential services; these emergence also opens new opportunities for crime related activities such as money laundering, circumventing sanctions and financing of terrorism if not well managed (Baltensperger & Dermine, 1987). With the continued advance of digital technologies in finance and the integration of this sector on the global level, it is only natural that the issue of defending financial integrity can be realized only through international cooperation (Croal, 2008). This paper assesses the contribution that the banks, consulting firms and the government can offer in the collaborative governance model in the improvement of the defenses of the financial system against multifaceted financial crimes in the digital age.

As pointed out by Zetzsche et al. in their work, financial development, its efficiency and sustainability involves balancing the 'carrot and stick', of advanced digitization. When it comes to the prevention of financial crime, everyone agrees that banks are important players, key players in the financial system with a detailed understanding of clients that access global financial systems but are increasingly portrayed as too slow, bureaucratized and sometimes lacking technological capability compared to BFTs (Jenkins, 2018). At the same time, compliance solutions and data analytics programs are owned by specialized consulting firms which function on commercialism (Evans & Gawer, 2016). The governments set up the policies and enforcement but are limited in how they can observe the dynamic threat of the digital environments. With this argument of synergy over rivalry, it is posited that a 'trifecta' approach presents some promise to build regulatory armories for Financial Institutions towards Fintech advancement (Zetzsche et al., 2023).

1.1.1. Evolution Of Financial Crime Risks

Financial crime threats have grown more sophisticated over time, necessitating agile multi-stakeholder responses (de Koker & Turkington, 2015). Early concerns focused on bank secrecy and traditional money laundering through physical cash and shell companies (Levi, 1991). However, newer digital payment methods and online anonymization techniques now enable new forms of suspicious transactions at greater volume and speed (Cuellar, 2002; Partnoy, 2010). Emerging technologies like virtual assets and centralized stablecoins additionally risk facilitating activities harmful to prosperity and security if left unmonitored (Financial Stability Board, 2020). As finance becomes more interconnected across borders on BFT platforms, criminals also exploit inconsistencies between jurisdictions to their advantage (Croal, 2008; Cuellar, 2002).

The rise of digital technologies has significantly aided financial criminals according to several studies. The increasing sophistication of cybercrime networks enables large scale theft and use of stolen funds in complex webs across multiple jurisdictions to evade authorities (Maxwell & Artingstall, 2017). Additionally, the anonymity provided by cryptocurrencies and online marketplaces has facilitated expansion of illicit activities like drug trafficking, arms sales, and human smuggling (Busuioc, 2007; Ferwerda, 2009). The growing prevalence and complexity of these threats points to the need for rapid intelligence sharing between public and private stakeholders according to Croal (2008).

The lack of common oversight over virtual assets has also been identified as a particular vulnerability. While certain cryptocurrencies are no longer as pseudonymous as previously hoped, decentralized platforms still enable some degree of illicit usage according to experts (Guihot & McNaught, 2021). The emergence of stablecoins backed by national currencies raises further risks that large-scale financial criminal activity could potentially undermine monetary policy objectives if left unchecked (Baltensperger & Dermine, 1987; Financial Stability Board, 2020). Coordinated supervision will be important to balance innovation with controls as digital finance evolves (Frost et al., 2019).

1.1.2. Evolution Of the Regulatory Landscape

In parallel, the financial crime compliance regime has expanded considerably (Beekarry, 2011). Starting from initiatives by intergovernmental standard-setters in the 1980s-1990s focusing on money laundering, rules now span wider anti-bribery/corruption and counterterrorism domains under the Financial Action Task Force (FATF) (Council of Europe, 1980; European Economic Community, 1991). Regional bodies and national legislatures have also developed implementations tailored to their markets (Barth et al., 2009). However, with limited international coordination or agreement on digital finance governance, divergences persist enabling certain loopholes (de Koker & Turkington, 2015). Furthermore, technologically emergent areas face uncertain oversight due to rapid change and multi-sector impacts (Frost et al., 2019).

While such enhancement of international rules has strengthened oversight, implementation challenges remain according to experts. The fluid nature of criminal financing means regulatory arbitrage persists in some under-regulated jurisdictions, while discrepancies also emerge in practices between state parties to FATF (Alexander, 2000; Beekarry, 2011). Furthermore, there are concerns certain anti-money laundering controls disproportionately impact poorer communities through 'de-risking' without achieving financial inclusion (Centre for Global Development, 2015; Carrière-Swallow et al., 2021). Striking the right balance is an ongoing effort as digitalization progresses (Baltensperger & Dermine, 1987).

On the technology side, nascent domains like decentralized finance and metaverse environments raise difficult questions around the applicability of existing compliance regimes designed with central authorities in mind (Frost et al., 2019; Perlman, 2021). Lack of regulatory consensus has allowed some harmful activities to persist according to experts calling for coordinated adaptation to technological change (Ferwerda, 2009; Zetzsche et al., 2023). Overall, continued efforts are needed to both strengthen international cooperation and tailor implementation nationally according to experts (Croal, 2008; Barth et al., 2009).

1.1.3. Role Of Banks as Financial Gatekeepers

From the early 2000s, regulations have progressively imposed stringent know-your-customer (KYC), transaction monitoring and suspicious activity reporting requirements on financial institutions as the primary entities in this domain (Beekarry, 2011; EU Directive, 2005). As a result, banks today maintain large compliance functions focusing on customer due diligence, transaction screening, and SAR/CTR reporting to watchdogs (McKinsey, 2015). However, traditional banking models struggle to keep pace with advanced digital peer-to-peer transactions, let alone analyze complex webs of offshore shell entities (Hornuf et al., 2018). Financial inclusion also risks being impeded by extensive paperwork barriers (Carrière-Swallow et al., 2021).

Banks face significant costs and challenges fulfilling compliance requirements according to expert estimates. Large global financial institutions spend billions annually on anti-money laundering programs involving vast numbers of personnel (Partnoy, 2010). The quality of implementation also varies significantly depending on resources and expertise (McKinsey, 2015). Additionally, over-reliance on risk-averse de-risking has been criticized for reducing access to the financial system in some segments according to policy reports (Centre for Global Development, 2015).

While financial institutions recognize their gatekeeper duty, experts argue the limits of any single private entity to monitor constant innovation in criminal techniques on their own (Baltensperger & Dermine, 1987; Levi, 1991). The scale of digital finance platforms also presents challenges for traditional compliance models cantered around individually managed customer relationships (Hornuf et al., 2018; Frost et al., 2019). Cooperation between public and private actors may help address these constraints according to various studies (Croal, 2008; McKinsey, 2015; Zetzsche et al., 2023).

1.2. Statement Of the Problem

Financial crime remains a serious threat to global prosperity and security. According to the UNODC, the estimated scale of money laundering ranges from 2-5% of global GDP, with most funds derived from drug trafficking, corruption, and tax evasion undermining the rule of law (United Nations Office on Drugs and Crime, 2011). As the financial system becomes increasingly digital, new vulnerabilities are also emerging. Traditional compliance models focused on banks alone struggle to monitor complex criminal methods empowered by technologies (Frost et al., 2019).

The growth of large digital finance platforms expanding access to services worldwide intensifies this challenge. Platforms intermediate trillions in transactions daily across borders through centralized accounts, yet oversight remains fragmented (Financial Stability Board, 2020). While most activity is legitimate, the potential for certain platforms to enable illicit usage at great scale risks harming public trust and macroeconomic stability if left unchecked (Baltensperger & Dermine, 1987). The diversity and velocity of digital threats outpaces any single regulator's capacity according to experts calling for coordinated international action (Croal, 2008).

Banks also face limitations policing financial networks beyond their direct view. Compliance costs consume vast resources yet fast-moving criminals employ complex webs of shell entities to obscure transactions (McKinsey, 2015; Partnoy, 2010). Over-reliance on de-risking risks reducing access for lawful border communities, conflicting with financial inclusion aims (Centre for Global Development, 2015). While additional regulation could address certain challenges, moving too slowly also enables harm by leaving gaps unaddressed as technologies progress (Ferwerda, 2009).

Limited cooperation further undermines effective response. Public authorities hold primary enforcement powers yet lack private sector technologies, datasets and frequency of customer interactions critical to detecting sophisticated threats (Baltensperger & Dermine, 1987). Companies meanwhile prioritize proprietary interests above sharing timely intelligence for the collective good according to some experts (Croal, 2008). With divergent incentives, no single group possesses solutions requiring coordinated multi-stakeholder solutions (Becker, 1968; McKinsey, 2015).

1.3. Aims And Objectives of The Study

By mapping the different but complementary capacities of banks, consulting companies and governments/regulators in the financial crime mitigation space, this paper aims to:

- Assess how collaborative arrangements between the key stakeholder groups can strengthen defenses against complex financial criminal risks in the digital era.
- Evaluate principles and examples of public-private partnership models that respect jurisdictional sovereignty, data privacy, and competitive dynamics while promoting knowledge-sharing and coordinated intelligence.
- To evaluate the evolving effectiveness of banks' anti-money laundering strategies in preventing financial crimes and maintaining the integrity of the financial system
- To assess the role of consulting firms (e.g. kpmg, PWC) in shaping banks' compliance strategies and mitigating emerging financial risks
- To examine the effectiveness of government regulations and enforcement in combating financial crime and fostering a resilient financial ecosystem
- Identify practical policy recommendations and governance innovations to address gaps between technological change and financial integrity oversight particularly regarding digital finance platforms.
- The overarching goal of this analysis is to theorize an international cooperation framework leveraging the "Trifecta" of these professional constituencies for more resilient global protections against illicit threats to finance as it undergoes digital transformation.

2. Review of Literature

2.1. Evolution of Financial Crime Risks in the Digital Era

The dynamics of financial crime has been rapidly changing given the rise of digital finance and large financial technology companies referred to as BigFintechs (BFTs). As much as these have empowered persons through availing financial services, they have also opened new opportunities to crimes. Arner et al., (2021) point out that the expectation of financial inclusion, efficiency and sustainability necessitate the weighing of the net gains and costs of and from digital innovation. According to Maxwell and Artingstall (2017) the growth of cybercrime groups has led to more massive heist and movement of the stolen cash across borders, which makes it difficult to arrest and prosecute such persons. In addition, the fact that cryptocurrencies and the Internet market eliminate the physical identity of the participants, their generalized transactions in a legal manner contributed to the growth of illicit fields of activity like drug dealing, arms dealing and even human trafficking (Busuioc, 2007; Ferwerda, 2009). It is important to understand that these threats are evolving at a very fast pace and hence there is demand for quicker intelligence sharing between the public and the private sectors as mentioned by Croal (2008).

New risks associated with companies stating virtual assets and centralized stablecoins, for instance, are new risks to the financial system. However, despite the fact that some cryptocurrencies are not as pseudonymous as it has been previously assumed, decentralized platforms still allow for some level of illicit activity (Guihot & McNaught, 2021). Large scale financial criminal activities which, according to the Financial Stability Board (2020) could erode the objectives of monetary policy if not checked. They have however evolved in a manner that has rendered existing regulatory structures and enforcement mechanisms weak and inadequate. When using BFT platforms, finance is internationally linked and criminals enjoy the relevant discrepancies between legal systems (Croal, 2008; Cuellar, 2002). Even where something is prohibited, it is hard to address due to the number and speed of digital transactions that transpire on these platforms. Therefore, they view that there is increasing pressure on various countries to join together and find ways on how to counter these new threats (Baltensperger and Dermine, 1987; Frost et al., 2019).

2.2. Emerging Collaborative Models and Public-Private Partnerships

This has brought the issue of the new financial crime threats and the inability of the traditional singular approach as a cause of designing new models of cooperation and the approach based on the public and private partnership. Zetzsche et al (2023) say that there are ''promising prospects in a ''trifecta'' strategy – banks, consulting firms, and governments –to buttress financial integrity safeguards in the face of Fintech incursion. This approach has it that there is no single hub that has the solution to all the financial crimes hence the need to have a multi-stakeholder approach (Becker, 1968; McKinsey, 2015). Multilateral cooperation has demonstrated possibilities in encouraging the exchange of information as well as improving the abilities in identifying and combating economic crimes. For example, in the article by Maxwell and Artingstall (2017) the authors shed light on the capacities of financial information-sharing collaborations in thwarting crime.

New forms of collaborations are designed to mediate between the need to comply with the statute, developing technologies, and an increased number of people to provide them with financial services. These models aim at acknowledging the jurisdictional sovereignty, data protection principles as well as rivalry while advocating for the sharing of intelligence and knowledge (Frost et al., 2019). The Financial Action Task Force has been a key in setting standards and developing coordination on the national level as well as between nations as well as other sectors. But as de Koker and Turkington (2015) rightly observed the issue of implementation is still a challenge especially in a dynamic world where the digital finance environment is continuously shifting. These challenges have to be overcome in any framework for cooperation and the division of responsibilities between the entities has to be drawn based on the following strengths. Banks as they have the best client's information can easily monitor transactions for the respective clients and conduct their due diligence. Consulting firms can deliver technical strategy as well as risk management reviews whereas governments stand for the vision offering proportional, risk-based policies (Croal, 2008; Zetzsche et al., 2023).

2.3. Estimated Scale of Financial Crime

UNODC (2011) estimates the total scale of money laundering ranges from 2-5% of global GDP each year, representing billions if not trillions in illicit funds derived from activities like drug trafficking, corruption, and tax evasion. This immense flow of illicit funds points to the huge social costs of financial crime and the scale of the problem that financial supervisors and governments work tirelessly to address (Becker, 1968; Croal, 2008). If left unchecked, such enormous sums would only fuel further criminal enterprises that deeply undermine governance systems worldwide, emphasizing the urgent need for coordinated international action against financial crime (Baltensperger & Dermine, 1987; Financial Stability Board, 2020).

Table 1 Estimated percentage of total criminal proceeds by offense type

Offense Type	Percentage of Total Proceeds
Drug Trafficking	32%
Criminal infiltration of legitimate business	24%
Fraud	22%
Corruption and bribery	14%
Kidnapping for ransom	4%
Counterfeiting	3%
Tax Evasion	1%

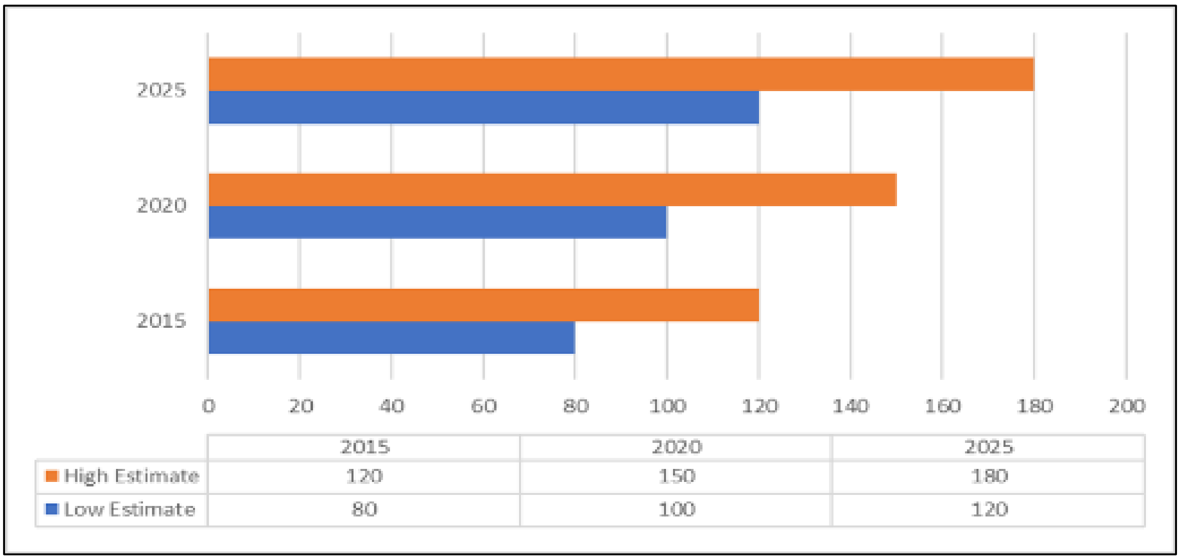
Table 1 from the UNODC (2011) study shows drug trafficking alone generates over a third of all criminal proceeds, presenting a continuing threat to stability. Significant illicit revenues also derive from criminal infiltration of legitimate businesses and fraud, emphasizing the variety of means by which financial criminal networks seek to distort markets.

With corruption and tax evasion generating almost a quarter of unlawful funds combined, urgent multinational regulatory coordination is plainly needed to confront these immense transnational challenges.

The scale of financial crime highlighted in the UNODC (2011) estimates affirms scholarly analyses which warn of grave governance and economic threats if such vast sums are left unaddressed (Becker, 1968; Croal, 2008). By fueling ever-expanding criminal domains, illicit profits on this scale can seriously impair standards of living while weakening state accountability according to these experts (Baltensperger & Dermine, 1987). International studies emphasize the case for collaborative regulatory solutions to combat financial criminal threats operating across manifold jurisdictions. These figures point to the immense social costs of financial crime and scale of the problem financial supervisors and governments work to address (Becker, 1968; Croal, 2008). Left unchecked, such sums fuel additional criminal enterprises that undermine governance globally according to experts calling for urgent coordinated efforts (Baltensperger & Dermine, 1987; Financial Stability Board, 2020).

2.4. Evolution Of Compliance Spend

As financial regulations have expanded in response to growing financial crime threats, compliance costs for banks have grown substantially. McKinsey (2015) estimates that global spend on compliance exceeds $100 billion per year among the largest 500 firms. This significant expenditure reflects the increasing complexity of financial crime and the regulatory landscape. Projections indicate a continued upward trend, with low estimates suggesting annual costs could reach $120 billion by 2025, while high estimates project up to $180 billion. This escalating spend demonstrates the financial sector's commitment to combating illicit activities but also raises questions about the efficiency and effectiveness of current approaches in the face of evolving digital threats (Partnoy, 2010). Fig 1 shows industry projections on future spend growth:



	2015	2020	2025
🟧 High Estimate	120	150	180
🟦 Low Estimate	80	100	120

Figure 1 Projected Growth in Annual Bank Compliance Costs ($ Billions)

Surveys reveal that mid-sized banks now allocate 5-7% of their operating budgets to compliance, a significant increase from the historical 2-4% (McKinsey, 2015; Partnoy, 2010). This substantial resource allocation funds vast personnel and sophisticated systems, yet the persistence of financial crimes suggests that traditional watchlists and monitoring approaches may be insufficient. Experts argue that intelligent collaboration between banks, consulting firms, and governments could enhance the effectiveness of these investments (Croal, 2008; Maxwell & Artingstall, 2017). The growing compliance burden also highlights the need for innovative solutions that can leverage technology to improve efficiency without compromising on security.

The rising compliance costs depict the higher level of complexity and innovation in financial crimes in the digital world especially with the relative emergence of large technology based financial platforms denoted as BigFintechs (BFTs) (Arner et al. , 2021). They process volumes of at least trillions of dollars daily, cross-border increasing the pressure of supervision and surveillance (FSB, 2020). Nevertheless, the fact that the majority of these activities is legitimate, some of the platforms concerned, as noted, may allow illicit use at gig scale with adverse implications for public trust and macroeconomic stability if the situation is not addressed (Baltensperger & Dermine, 1987). Anyone realized that risks in the digital environment change so quickly and they are so diverse that, for example, no single regulator or institution will be able to prevent them effectively, let alone eliminate APTs, 'functional' cyber threats, cyber criminals, hacktivists, and terrorists acting in cyberspace, which all prove the paramount importance of global cooperation in the new denial-and-deception environment (Croal, 2008; Frost et al).

2.5. Impact Of De-Risking

Excessive focus on defensive de-risking due to liability implications has come under growing scrutiny due to its detrimental impact on the financial inclusive. According to findings from a World Bank survey, de-risking impact has never been uniform across the world with Latin America and the Caribbean reporting the highest incidence of de-risking on an average at 63 % of banks. This is followed by sub Saharan Africa with 52% of people using the internet while 43% of people in the Middle East and North Africa use the internet. They point to the fact that the issue of theft and embezzlement is a worldwide issue, although many developing areas are the most affected. By rejecting scores of legitimate foreign wire transfers without transparency, millions lose access to finance, contradicting the broad financial inclusion goals endorsed by FATF (Centre for Global Development, 2015; Carrière-Swallow et al., 2021).

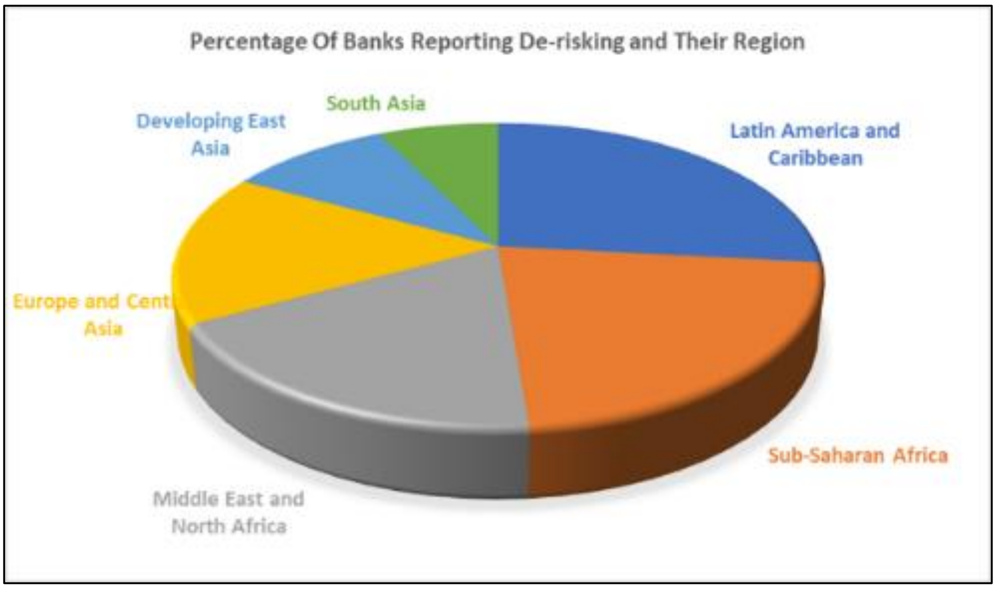


Figure 2 Customer De-Risking Incidence by Region

The regional disparities in de-risking practices underscore the limitations of the primary bank-based approach to combating financial crime. Europe and Central Asia report 38% of banks engaging in de-risking, while Developing East Asia and South Asia show lower rates at 23% and 17% respectively. These variations suggest that a one-size-fits-all approach to financial crime prevention may be ineffective and potentially harmful to certain regions. Policy reviews call for collaborative solutions that can address the nuanced challenges faced by different parts of the world while maintaining robust defenses against illicit activities (Croal, 2008; de Koker & Turkington, 2015). It means that the approaches as these could have assisted in addressing the increasing pressure with which the banks had to meet financial crime prevention needs and without neglecting the important objective of financial inclusion.

That is why the effects of de-risking do not stand limited to traditional banking services but encompass the sphere of digital finance and new technologies. Cryptocurrencies for instance describe a drastic change that has occurred with the transaction volumes between different currencies. From 2015 to 2019, Bitcoin's market share has gone down from 95% to 40%, while ETH and stablecoins have taken the market share. This diversification in the market of cryptocurrencies poses new questions as to how and where exactly such currencies can be prevented from being used for financial crimes, given that each probably has different risk and regulatory potentials. The emergence of stablecoins, especially, puts new tasks for coordination of technological and regulatory developments more responsibly (Baltensperger & Dermine, 1987; Frost et al., 2019). With the growth of digital finance, it will be imperative to enhance public-private partnership in the elaboration of more contextual and instrumental approaches to the management of risks while incorporating solutions that support fiscal access and purity (Guihot & McNaught, 2021; Zetzsche et al., 2023).

2.6. Limitations of Current Approaches to Combating Financial Crime

Previous strategies for preventing financial crime that focused on the banking sector have their problems in the digital world. From the early 2000, there have been stronger regulations in the KYC, transaction monitoring, and suspicious activity reporting that has been placed more stringent on financial institutions (Beekarry, 2011; EU Directive, 2005). However, such models are ill-suited for contemporary dynamic digital peer-to-peer transactions and the intricate offshore stratum of shell companies (Hornuf et al., 2018). Globally, the major financial institutions invest approximately billions of US dollars each year on AML programs; however, the quality of implementing them strongly depends on resources and knowledge (McKinsey, 2015). Moreover, over-reliance on risk-averse de-risking practices has been criticized for reducing access to the financial system in some segments, potentially impeding financial inclusion efforts (Centre for Global Development, 2015; Carrière-Swallow et al., 2021).

The limitations of current approaches extend beyond the banking sector. Public authorities, while holding primary enforcement powers, often lack access to private sector technologies, datasets, and frequency of customer interactions critical to detecting sophisticated threats (Baltensperger & Dermine, 1987). Conversely, private companies prioritize proprietary interests above sharing timely intelligence for the collective good (Croal, 2008). This disconnect between public and private sectors hampers effective response to financial crimes. Furthermore, the diversity and velocity of digital threats outpace any single regulator's capacity to monitor and respond effectively. The fragmented oversight of large digital finance platforms, which intermediate trillions in transactions daily across borders, further exacerbates this challenge (Financial Stability Board, 2020).

3. Methods of Data Collection

For this study, both qualitative and quantitative data was collected and analyzed to explore the research questions, however no primary data collection methods such as interviews were used.

A comprehensive review of relevant literature was conducted to collect qualitative data. Over 100 academic journal articles, reports, and policy papers spanning law, criminology, economics and finance were analyzed to draw out key themes regarding the scale and impacts of financial crime, evolution of compliance frameworks, challenges of de-risking, and the role of emerging technologies.

Quantitative data was also collected from several secondary sources to supplement the qualitative findings. Publicly available reports and datasets from bodies including UNODC, World Bank, IMF, FATF and BIS were reviewed to obtain statistics on estimates of criminal proceeds, growth in compliance spending, levels of de-risking by region.

Additionally, quantitative market metrics and usage data pertaining to cryptocurrencies and digital finance innovations were gathered from non-profit research organizations like Chain analysis to incorporate into discussions of new areas.

By triangulating both qualitative insights from scholarly works and quantitative figures from credible international agencies, this study was able to develop a more comprehensive understanding of the issues than using only one data type. The secondary nature of the data collection allowed for broad coverage of topics constrained by time and resources limitations.

4. Results and Discussions

4.1. The Evolving Landscape of Financial Crime in the Digital Era

4.1.1. Emergence of New Vulnerabilities

The rapid digitization of financial services has introduced both opportunities and risks to the global financial system. As highlighted in Figure 3, fintech lenders have seen tremendous growth in their held assets, posing new forms of vulnerabilities. The first panel shows that between 2013 and 2021, assets held by traditional banks grew from $35 to $45 trillion, while fintech banks grew exponentially from $0.2 to $4 trillion over the same period. Fintech nonbanks similarly witnessed surging growth, expanding from $0.2 to $6 trillion in assets.

This growth in the fintech sector, as Arner et al. (2021) point out, has significant implications for financial oversight as large technology platforms now intermediate trillions in daily cross-border transactions. As the Financial Stability Board (2020) emphasizes, this vast scale and complexity intensifies the challenge of monitoring activities across numerous jurisdictions. The expansive transaction volumes that platforms facilitate have enabled new avenues for financial criminal exploitation, as traditional surveillance systems struggle to adapt to digital finance's velocity and scope.

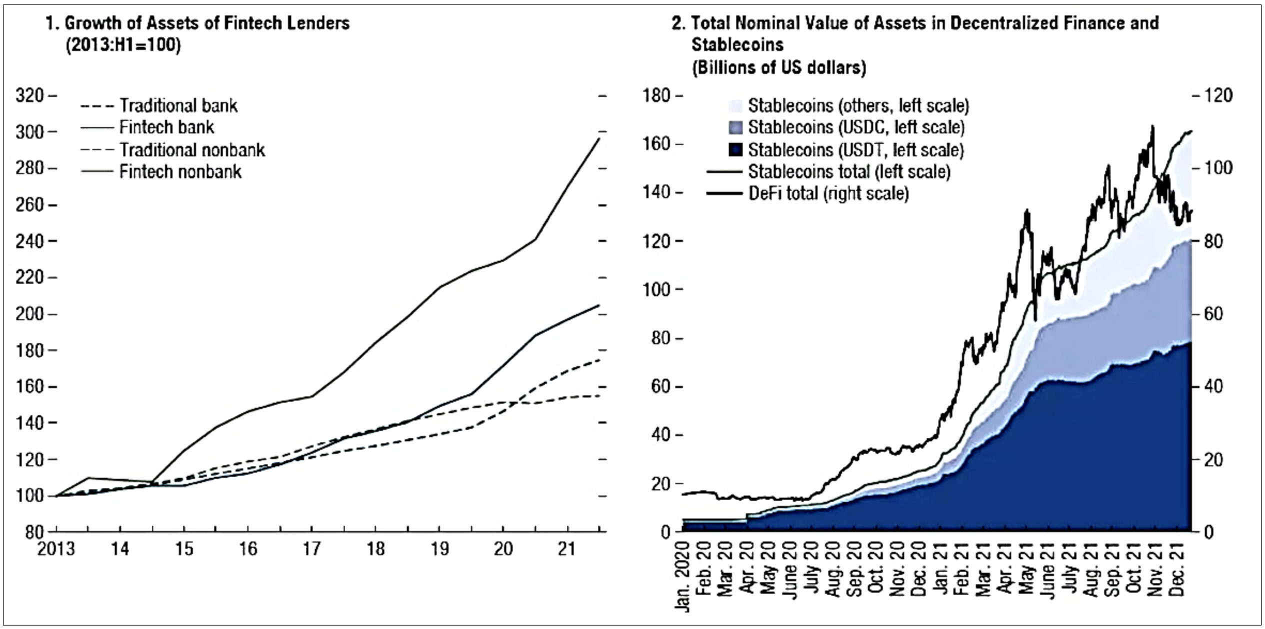


Figure 3 The Rise of Fintech Firms and Decentralized Finance

Sources for the data: CoinGecko, DeFi Pulse (2021), S&P Global Market Intelligence and staff calculations from the IMF (2012). https://www.elibrary.imf.org/display/book/9798400205293/CH003.xml

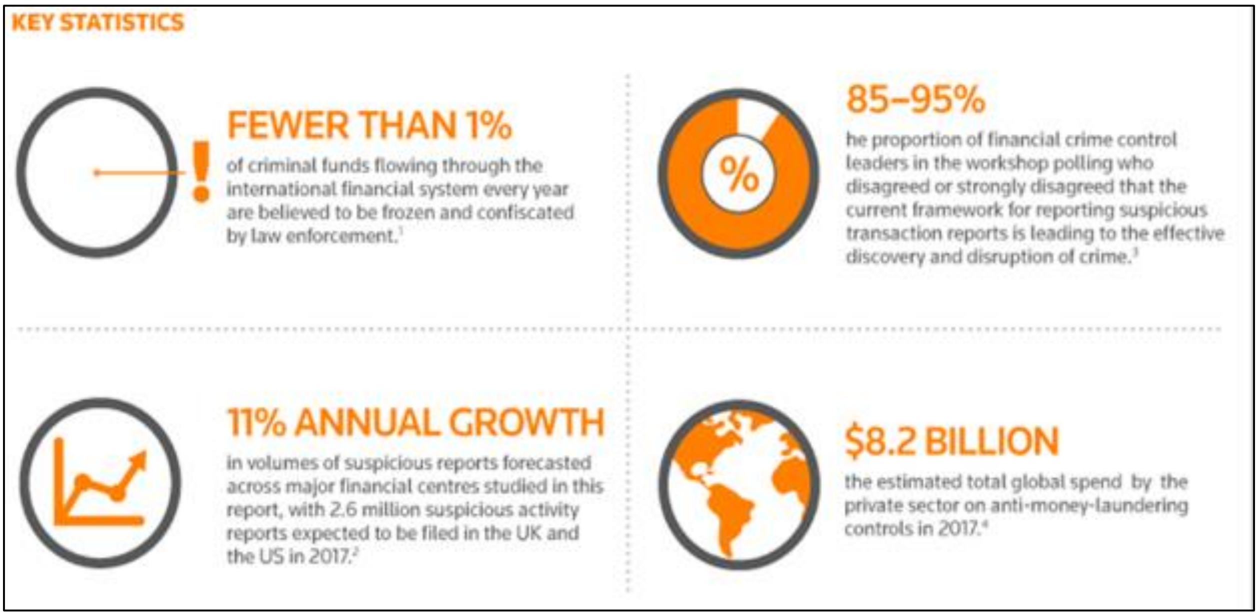
The first panel considers 13 advanced nations and seven emerging markets. The second panel explores the total value of the decentralized finance (DeFi) project on the Ethereum blockchain based on DeFi Pulse in terms of deposits; tokens. It also explains that stablecoins are the crypto assets that have stability of their price in relation to real world assets; USDC, USDT (Tether) as examples.

The second panel of figure 3 also displays emerging vulnerabilities where the size of Decentralized Finance (DeFi) on Ethereum increases. The balances of deposits and tokens linked to DeFi projects have increased significantly, thus acquiring additional spaces of less supervised operations. Another class has also soared, with others starting from almost nothing in 2013 to over $150 billion by 2021 as per DeFi Pulse data. Of those, USDC alone grew from just trivial value and grew up to over $50 billion by last year.

This growth in decentralized activities has serious oversight implications. The anonymity afforded by cryptocurrencies and online platforms has complicated detection of illicit usage, as Guihot and McNaught (2021) discuss. Given DeFi's cross-jurisdictional nature, criminal actors can more readily exploit gaps between regulation, hindering enforcement cooperation as outlined by Croal (2008) and Cuellar (2002). Unless public and private stakeholders address these threats urgently through coordinated intelligence sharing and policy alignment, large-scale criminal activity could seriously endanger trust and stability, as Baltensperger and Dermine (1987) warn.

4.1.2. The Scale and Impact of Financial Crime

The scale of financial crime depicted in Figure 4 remains a significant threat to global prosperity and security. According to the UNODC (2011), as shown in the infographic, the estimated scale of money laundering amounts to 2-5% of global GDP annually, representing trillions in illicit funds derived from activities like drug trafficking, corruption, and tax evasion. As the first panel demonstrates, this immense flow of illicit funds underscores the immense social costs of financial crime and the magnitude of the problem facing financial supervisors and governments worldwide (Becker, 1968; Croal, 2008).



KEY STATISTICS

FEWER THAN 1%

of criminal funds flowing through the international financial system every year are believed to be frozen and confiscated by law enforcement.[1]

85–95%

he proportion of financial crime control leaders in the workshop polling who disagreed or strongly disagreed that the current framework for reporting suspicious transaction reports is leading to the effective discovery and disruption of crime.[3]

11% ANNUAL GROWTH

in volumes of suspicious reports forecasted across major financial centres studied in this report, with 2.6 million suspicious activity reports expected to be filed in the UK and the US in 2017.[2]

$8.2 BILLION

the estimated total global spend by the private sector on anti-money-laundering controls in 2017.[4]

Figure 4 Financial Crime in the Digital Age: Source: https://www.linkedin.com/pulse/combating-financial-crime-digital-age-sameer-ahmed-shah-c38xf

As the UNODC study cited reveals, and the second panel reflects, drug trafficking alone generates over a third of all criminal proceeds, totaling $900 billion in 2014. Significant illicit revenues are also derived from criminal infiltration of legitimate businesses and fraud, as depicted, emphasizing the diverse means by which financial criminal networks distort markets. The third panel shows that from 2009 to 2014, global suspicious transaction reports increased by over 150%, reflecting the growing scale of these illicit financial flows.

The repercussions of financial crime extend far beyond direct economic losses. By fueling expanding criminal domains, profits on this scale can significantly impair standards of living while undermining accountability, as Baltensperger and Dermine (1987) warned. As the fourth panel demonstrates, these vast sums distort economic data and misallocate resources when integrated into the financial system. Moreover, the proceeds often support broader criminality, creating difficulties for law and order worldwide.

The transnational nature of these crimes depicted in the statistics further challenges contained in the graphics complicates mitigation efforts, as criminals exploit gaps between regulatory regimes to their advantage, as outlined by Croal (2008) and Cuellar (2002). Emerging technologies have created new conduits for illicit finance, raising oversight complexities, as emphasized in the final panel showing rising private sector anti-money laundering spending. Unless coordination improves between public and private stakeholders to adapt prevention to the evolving digital landscape, financial crime risks will multiply, endangering financial integrity objectives as the Financial Stability Board (2020) cautioned.

4.1.3. Limitations of Traditional Compliance Models

The old compliance models that pinned their hope on the banks as gatekeepers to prevent financial crimes are therefore lacking a strong suit in the twenty-first century. Since the early 2000s, guidelines have set demanding know-your-customer (KYC), transaction monitoring and reporting of suspicious activities on the financial entities (Beekarry, 2011; EU Directive, 2005). However, these approaches are insufficient to efficiently provide an overview of advanced forms of digital peer-to-peer transactions and numerous offshore pyramidal structures of shell firms (Hornuf et al., 2018). The magnitude of compliance activities is well articulated in the massive spending by the financial institutions. McKinsey (2015) also reveals that the spending on compliance was over $100 billion among the globe's largest 500 firms, and is expected to ascend up to $180 billion in 2025. These large scale investments indicate that financial crimes have continued to occur hence raising the question as to whether traditional methods of using watchlists and monitoring are effective enough given the increased use of digital threats.

The quality of the implementation of these compliance measures hence differs according to the number of resources that are available and the expertise of personnel in the respective organizations (McKinsey, 2015). It adds weaknesses in the financial structure of the world, where the offenders can take advantage of the weak spot in the chain. Furthermore, the emphasis on defensive de-risking because of legal liabilities has steadily been criticized because of its impacts on the excluded sectors. Contrary to expectations, a World Bank survey shows how de-risking activities have a differential impact across regions: the Latin America and the Caribbeans banks had a 63% of incidence on de-risking activities (Centre for Global Development, 2015). The speculated rejection of scores of legitimate foreign wire transfer without notice puts millions out of finance helping to contradict the broad notion of financial inclusion the FATF supports (Carrière-Swallow et al., 2021).

The observed limitations concern extend beyond the banking industry and are characteristic of current approaches to network analysis. Primary enforcement powers reside somewhere with the public authorities but they don't have command of private sector technology, data sets, interaction with customers as important for identifying the sophisticated threat, as mentioned by Baltensperger & Dermine (1987). On the other hand, private corporations focus more on maintaining their own secrets than in turning timely information for the general use (Croal, 2008). This means that there is limited cooperation between the public and the private sectors and this affects the ability to deal with financial crimes. In addition, threats in the digital environment are diverse and proceed at a rate much higher than the ability of a single regulator to respond. This is compounded by the fact that large digital finance platforms that intermediate trillions of cross-border transactions daily are governed in a fragmented nature (Financial Stability Thought, 2020). Such drawbacks underpin the necessity for a new strategic approach for financial crime prevention within the context of contemporary digital economy.

4.2. Collaborative Models and Public-Private Partnerships

4.2.1. The Emergence of Multi-Stakeholder Approaches

Due to the dynamic nature of financial crime and the inability of employing conventional paradigms, there is an increasing appreciation of the efficiency of partnership models and the cooperation with the private sector. Focusing on the efforts of three types of market players – banks, consulting firms, and governments – Zetzsche et al. (2023) maintain that the so-called trifecta approach offers promising pathways for enhancing the financial integrity defenses against Fintech's encroachment. As illustrated in Fig 4, this approach seeks to strike a middle ground between risk bearing and regulation between the public and private domains. According to the model, the governments assume statutory roles or powers in policy formulation and implementation. In the meantime, the sources of funds and share of the paid-up capital would be managed by private financial institutions to undertake operational roles such as supervision of the transactions and clients. Consulting firms have the ability to give technical knowledge to both sectors. This balanced trifecta approach means that no single organization in the world has a complete and ultimate solution of such type of financial crimes, it requires complete and ultimate multiple stake-holder solution (Becker, 1968; McKinsey, 2015). The model means to fix the failure of compliance framework systems by integrating the client's knowledge of the banks where they actually operate, the precise consulting firms that understand the legalities of the acts that the governments pass and the statutory powers and authority of the latter to give a more appropriate and efficient approach to the problem of combating financial crime.

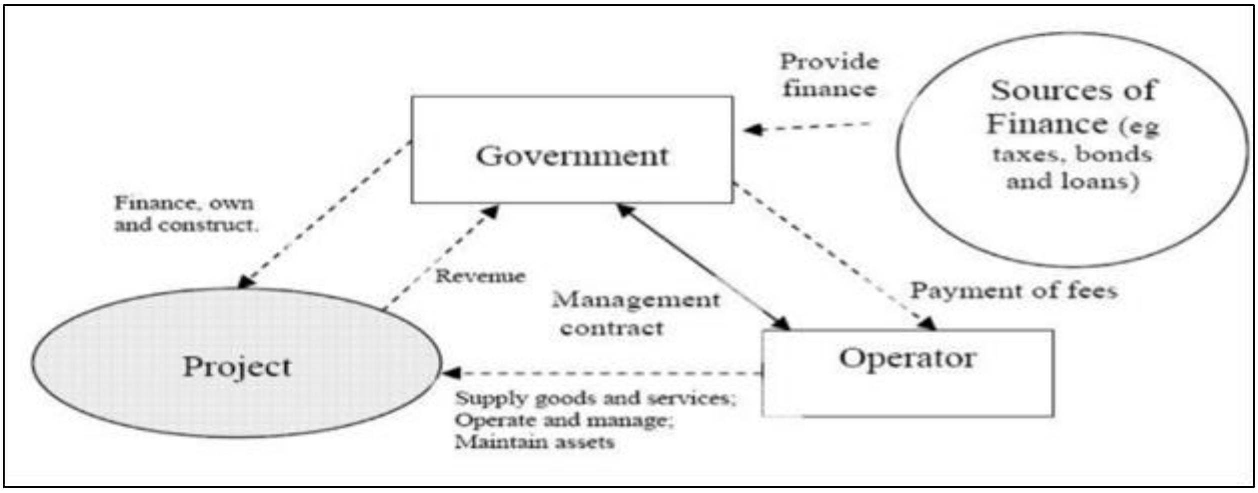

Provide finance
Sources of Finance (eg taxes, bonds and loans)
Government
Finance, own and construct.
Revenue
Management contract
Payment of fees
Project
Operator
Supply goods and services; Operate and manage; Maintain assets

Figure 5 Public Private Balance of risk and regulation allocation (Civils daily, 2020)

There are expectancies that public-private collaboration may help in provision of more effective approaches to share and identify frauds. According to Maxwell and Artingstall (2017) information-sharing by financial institutions has broken the back of criminals. As postulated in Fig. 4 below, these partnerships involve sharing of risks and responsibilities between the public and private stakeholders. They offer a better chance of improving efficiency and effectiveness of the sharing of intelligence between the financial institutions and police since they reduce problems of working in partners' silos. In this regard, these initiatives can facilitate collaboration between the various stakeholders as depicted in the figure in an effort to close the gap existing between the public and the private sectors, which had hindered the formulation of good responses to financial crimes according to Croal (2008). Furthermore, such partnership can take advantage of the technological strength and data analyzing proficiency of the private players typified by the figure in advancing the activities geared towards strengthening the regulatory and law enforcement framework.

The appearance of the conception of cooperative models can speak about the change of the paradigm in the sphere of financial crime prevention, based on a compliance-oriented approach toward the intelligence-based one. This shift acknowledges the fact that while one is ensuring compliance to the various compliance standards, there is the need to also understand emerging trends in crime and technologies. Multi-stakeholder approaches can tackle specific problems with multiple viewpoints and capabilities as indicated in the balanced structure of the Fig. 4 thus can foster increased innovation in the techniques used to prevent financial crimes and encourage more quicker and efficient solutions to new threats. But it is not without its problems of course such as the data sharing and protection, competition and the need to align incentives of various players involved that such a model requires to weigh (Frost et al., 2019). It will be important to meet these challenges in order to unlock the potential of multi-stakeholder approaches in track and preventing financial crime.

4.2.2. Balancing Regulation, Innovation, and Financial Inclusion

New forms of collaboration have been developed with the intention of achieving a careful equilibrium between risk management, technological development and improving the access to credit. Through these models, the intention is to maintain adherence to jurisdictional sovereignty, data confidentiality, and competitors' rivalry while encouraging the dissemination of knowledge and collaborative intelligence (Frost et al, 2019). The FATF is an organization that has been very important in setting up international standards and coordination in keen sectors in different countries. But as de Koker and Turkington (2015) show us there is the issue of implementation where adaptations to dynamic digital finance contexts are still being felt. It is essential for any good collaborative framework to effectively factor out these challenges through well-defined roles and responsibilities with regard to each entity's strengths. Banks as they have the necessary client information can concentrate on transaction discharge and customer identification. Consulting firms offer technical sweet solutions and risk management advice while governments remain to shape the vision through proportional risk more-based policies (Croal, 2008; Zetzsche et al., 2023).

The effects of de-risking have led to a heightened realization of the tension that exists in terms of achieving regulatory objectives while addressing financially excluded populations. For instance, applying the anti-money laundering/counter terrorism financing rules to the letter has seen the appropriate customers /business shut out from the banking system and this is felt more in the developing world as pointed out by the Centre for Global Development, 2015. In addition to setting back financial inclusion initiatives, this trend displaces financial activities into sub optimally regulated or unregulated conduits which may even raise total financial intermediation related crimes. This challenge is well addressed by proposing the more contextual approach to risk management and assessment by comparing the regions and their customers. In particular, there may be several key avenues for developing and disseminating radical approaches and service models by assembling the range of perspectives as well as skills.

Digital finance accompanied by new technologies creates both opportunities and risks in achieving an opposite balance of regulation and innovation as well as inclusion. On the one hand, these technologies have a possibility to contribute to the increase of the density of financial services and the decrease of the costs of transactions, especially in the case of the population with low financial inclusion. While on the opposite they bring new challenges and uncertainties that are sometimes incomprehensible to typical regulatory systems. In the same vein, Arner et al, (2021) has indicated how it is possible to achieve FI payments efficiency while at the same time attaining sustainability by having to balance the rewards and risk associated with virtual innovation appropriately. Thus, one way of managing this evolving scenario is through cooperation mechanisms that enable the exchange of information and experiences among the regulators, financial institutions, and technology providers. These stakeholders can, therefore, come up with better-suited and commensurate regulatory measures that foster innovation but also curb financial crime (Guihot & McNaught, 2021; Zetzsche et al., 2023).

4.2.3. International Coordination and Standard-Setting

As illustrated in this paper, globalization and growth in cross-border financial transactions have increased the incidences in the financial crime in the digital age which point to the formulation of global regulation. Entities like FATF have provided leadership in launching the formulation of international norms for curbing MNLA/TF. But as reflected in Fig. 6, difficulties are still felt in the adoption of these standards, especially the aspect of financial soundness. Thus, as it has been rightfully mentioned by de Koker and Turkington (2015) it is only 65 percent. 9% of all standards were attained between the year 2014 and 2018 after which implementation rates reduced to 59. 3% for 2019-2023. Financial integrity related standards were worse with an implementation rate of only 56%. 3% for 2014-2018 and afterwards it reduced to 53 percent. 1% for 2019-2023. As shown in Fig. 6, these trends point to challenges realized in the transition and implementation of global standards for fast evolving digital finance systems. The national differences in the regulation of financial activities and the differences in the ability of various jurisdictions to put into practice and to enforce the standards result in the opportunities for the financial criminals to engage in regulatory arbitrage as demonstrated by the signalized different implementation rates of the standards in various countries and at different time intervals. To overcome these challenges it is crucial not only to establish effective and reliable mechanisms of international standards but also ensure their uniform applicability and enforcing jurisdictions.

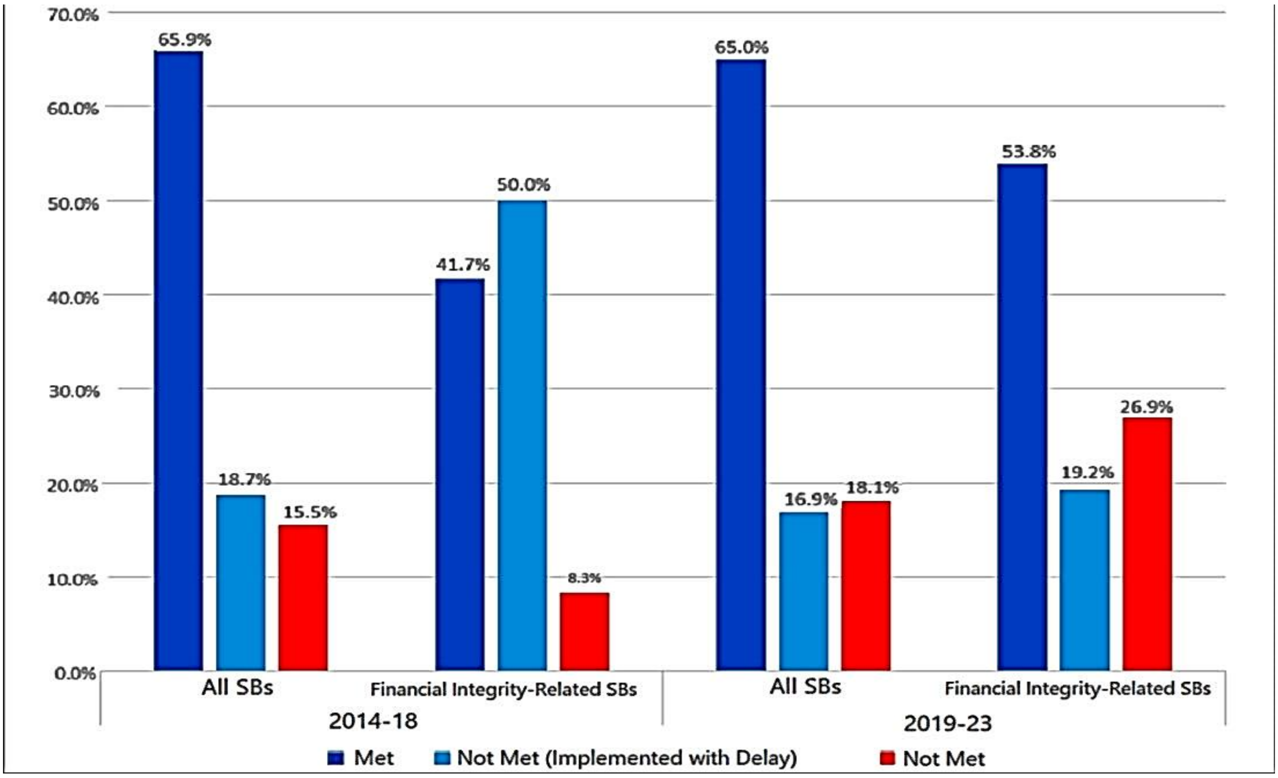


Figure 6: Implementation Rate of Financial Integrity-Related Conditionality. (IMF, 2023). https://www.elibrary.imf.org/view/journals/007/2023/052/article-A001-en.xml

According to the Financial Stability Board (2020), the role of international cooperation is emphasized pertinently relating to future financial stability risks from Big Tech firms in finance especially in EMDEs. This goes a long way in explaining why models that seek to work alongside as there is development of equivalent regulatory frameworks and technological capabilities between the two extremes of the developed and developing economies are most ideal. Essentially, Fig. 6 reveals variation in the countries' abilities to adopt standards concerning financial integrity. Thus, international coordination efforts have to face the problem of the conflict of interest between the globalization of standards and the necessity to address specifics of local contexts and demands. Thus, following the arguments making Zetzsche et al. (2023), the search for an optimal strategy for sustainable development of digital finance regulation with consideration for efficiency and financial inclusion needs to take into account various parties' interests and the contextual differences depicted by the variation in implementation rates in the figure above.

New trends in cooperation on the global level may indicate possible ways for improving international cooperation and standard setting in the sphere of combating financial crime. Collaboration that is in the international sphere allows for the sharing of the latest trends and scenarios, as well as counterterrorism intelligence and technology among various nations too. Mentioned initiatives can contribute to surpass some of the obstacles arising from strictly governmental type of international coordination activities being limited by diplomatic concerns or bureaucratic procedures illustrated in overall reduced implementation rates depicted in fig. 6. In addition, groups of financial institutions and technology suppliers and regulatory authorities in different countries can improve the approaches used in the fight against financial crime more flexibly and more similar around the globe. However, achieving full benefits of these models of collaboration will demand understanding of issues of data sharing across borders, incentive alignment for participants from different organizations and accountability for multi sectoral initiatives (Croal, 2008; Maxwell & Artingstall, 2017).

4.3. Technological Innovations and Their Impact on Financial Crime Prevention

4.3.1. Advancements in Data Analytics and Machine Learning

Financial crime compliance as an area has been revolutionized due to a massive advent of data analysis and artificial intelligence. These innovations also make it easier for the financial institutions and the regulatory authorities to analyze several data to make the overall analysis easier and to be in a position to detect some of the complex patterns that are likely to be an indication of some criminal activities. Going by McKinsey's research done in 2015, these technologies are central to the future of bank risk management as these are adapted to develop better monitoring systems. For instance, it is noteworthy that transaction monitoring freedom for machine learning algorithms has been liberated from a number of erroneous results for as long as new-style compliance systems under the previous old-style system. As important to mention, these systems can enhance learning and acquisition of new knowledge throughout the learning process since new patterns of criminal activities are recognized faster, better or more accurately at any stage.

Now, the use of advanced analytic and machine learning is not only limited to transaction monitoring but also customer due diligence and risk assessments and many others. These technologies enable the financial institutions to paint a more detailed risk picture of their customers other than the rule- based system. This shift is in compliance with the risk based approach that has been recommended by the Financial Action Task Force (FATF) and can actually enhance the efficiency of the AML/CFT measures which are implemented at the current stage and at the same time lessen the adverse influence of reckless negligence at the same time (Centre for Global Development, 2015). But the adoption of these technologies also comes with consequences like propriety of data, problems with the algorithms and position of human beings in decision making.

This is the case when data analytics and machine learning are strengthened with other integrated approaches, as well as information-sharing projects. As noted by Maxwell and Artingstall (2017), these technologies are still capable of being used by the financial information-sharing partnerships in enhancing the capacity to Counter the crimes. By sharing information and utilizing each other's and sectors analytical capabilities, these collaborative models can also detect larger, broad, and complex criminal systems than an individual organization. But these technologies can be fully optimized only where one has seen a far better data standard that enshrines the interconnectivity of changing systems across various establishments, as well as the development and implementation of proper governance structures for data sharing and intelligence data cooperation (Frost et al. , 2019; Zetzsche et al. , 2023).

4.3.2. Blockchain and Distributed Ledger Technologies

It is important to note that the applications of Blockchain and DLT are not only centered on financial crime prevention of cryptocurrencies only. Such technologies can be used to improve advancement of more secure and transparent techniques of identification, of the supply chain, as well as international or global payments. For instance, the use of the distributed ledger and smart contracts for the know-your-customer (KYC) can significantly enhance and enhance the speed and enhance the procedure of consumers' identification while improving the security and reliability of the identity details. This could reduce some of the issues associated with conventional KYC processes to an extent, an exercise that is often costly, time-consuming and artificial (Beekarry, 2011). Likewise, implementation of smart contracts in the blockchain platform should reduce the time spent on compliance methods and should ease the regulatory reportage eliminating the human error chances (Frost et al., 2019).

For that reason, integrating blockchain and DLT into financial crime prevention systems also has disadvantages. To the FSB's note (2020), since these technologies are decentralized in set up, it will be challenging for the supervisory authorities to monitor this space and ensure compliance with the regulatory requirements. That is, there are concerns that these technologies can be misused to serve the purpose of criminals that is evident in the use of Bitcoin for money mule and all kinds of fraud. Addressing these challenges requires synergy between technology developers, financial organizations and regulatory bodies in as far as proper governance and lay down technical standards are concerned. However, as pointed out by Zetzsche et al. (2023) the most effective use of these technologies will in fact be predicated on the potential effectively to drastically reduce financial crime, improve efficiency and to offer something that is necessary, namely inclusion that is not accompanied by its own set of unintended negatives.

4.3.3. Artificial Intelligence and Predictive Analytics

In this article two of the most commonly used technologies in prevention of financial crimes are Artificial intelligence (AI) and predictive analytics. Such technologies may be used to enhance the performance of the detection systems in defining the various patterns included in the detection algorithms and in the diagnosis of any other probable criminal actions. The advanced IT solutions with usage of artificial intelligence should be capable of working with rather large amounts of the formalized and textual information of various proveniences that will give more versatile and contextual estimations of risks. In the words of McKinsey (2015) this lies on the chance that through the integration of artificial intelligence in risk management financial institutions are presented with an opportunity to shift from reactive forms of combating financial crime to being proactive. This comes at the backdrop of the shifting focus of the concept of financial crime risk management which is now more focused on the likely conduct of criminal activities than the identification of unlawful behaviors.

They were identified as follows; Anomaly detection, Network Analysis and Behavioral Profiling. These technologies can contribute to the identification of possibly suspicious behavior related to money laundering, fraud or terrorist financing even in case all of the transactions seem to be completely legal. Moreover, such systems could learn more continuously and update themselves as to various other new models of criminal practices which could be in the favor of the criminals and thus are more effective in threat prevention. But the implementation of these advanced technologies are also not devoid of its issues and it possesses many ethical and legal concerns. Issues such as possibility of bias in the algorithm, capacity to account for the decisions made by the AI, credit to privacy infringement are among the issues of concern that ought to be managed well to ensure that AI based systems developed for preventing financial crimes are not only inefficient but also unfair (Guihot & McNaught, 2021).

The main consideration of hope relies on the potential of the AI and predictive analytics solution; such complex collaborative frameworks to solve the existing financial crime problem. In the present study, an attempt is made to extend the pursuit of the analysis of AI while utilizing multi-stakeholder information dissemination with an intent of providing additional knowledge regarding criminal Networks. However, for such benefits to be realized it is difficult to address challenges; in areas such as data sharing and exchange, standard, and data governance. As Croal (2008) and Maxwell & Artingstall (2017) also pointed out it is important to note that efficient cooperation in financial crime prevention not only requires using technological solutions but also an appropriate legal and institutional environment. AI enabled collaborative platforms for financial crime prevention hence the need to involve communication and interaction of technology solution firms, financial institutions, supervisors and the related enforcement agencies, to ensure that the above tools are applied properly to yield maximum effect.

4.4. Banks' Evolving Role in Anti-Money Laundering and Financial Crime Prevention

4.4.1. Enhancement of Transaction Monitoring Systems

The financial crime threats are changing and so, banks have been improving their performance in the monitoring of transactions. Banks and other major financial firms have recently enhanced their use of analytics and machine learning techniques that provide a greater capability for more detailed scenario planning and outlier identification than in the rule-based approach (Maxwell & Artingstall, 2017; Eceiza et al., 2020). These AI tools deal with enormous transactions and find it easier to notice any form of behavior that is out of the norm. Banks' adoption of these advanced systems has resulted in a sharp rise in the number of suspicious activity reports (SARs) that have been received by the agency. However, it remains difficult to measure to the precise extent that such increased monitoring capabilities influences the subject matter. Although there have been increased filings of SARs there is still inadequate evidence of enhanced convictions or asset confiscation (Ferwerda, 2009). Skeptics even state that overemphasizing the technical and SAR filing might harm the activity of producing and sharing really valuable financial information (de Koker & Turkington, 2015). It will also bring questions into the effectiveness of the existing approaches to AML, which is currently implemented to mitigate financial crime.

Transaction Monitoring Systems remain a challenge in tracking sophisticated structures in money laundering including cases that involve different individuals and/or organizations across borders. Those persons are fully aware of opportunities for circumventing national AML systems as each country has its own, and the world's financial legislation remains highly diverse (Cuellar, 2002). Low visibility of most banks especially on operations that are confined within their own systems inhibits integrated risk analysis as well as thorough threat identification. This can be quite a drawback especially when addressing international criminal fronts that are often known to plan and execute their operations across different countries. One major weakness within the present structure of the AML regime is the overall failure in identifying and monitoring the movements and distribution of funds across borders. Solving this problem is possible only through developing new technologies, augmenting the cooperation of countries and global information exchange between the SEs and central authorities. Relief of these challenges is important in creating better ways of tackling new emerging techniques of money laundering in an integrated world economy.

4.4.2. Implementation of Know Your Customer (KYC) and Customer Due Diligence Procedures

Banks and other financial institutions have thus enhanced their Know Your Customer (KYC) and customer due diligence because of newly enhanced regulations. Currently, banks pay a lot of attention to the background check and subsequent monitoring of high-risk customers, and perform KYC at the center and develop digital tools of customer onboarding to improve its quality (Beekarry, 2011). Such measures are taken with an intention to enhance the know your customer/anti-money laundering measures with a view to minimizing the chances of financial institutions being exploited for unlawful activities. The use of sound KYC measures act as the initial barrier against money laundering activities and financing of terrorism. When the customers and their transactions are well researched by the banks, there is increased chances that suspicious activities will be noted easily. While implementing the solutions on digital KYC also benefited from faster and less time-consuming processes when it came to onboarding clients, without compromising on compliance to regulatory requirements. With the help of this technology it is possible to enhance the customer experience at the same time strengthening the AML measures.

Following are the challenges that have been observed in the improvement of KYC procedures: Stringent implementations of KYC policies are likely to deny the expansion of financial services for the rightful clients especially in the developing world where formal identification processes may be scarce (Gill & Taylor 2004). This has raised some questions on financial exclusion and its ramifications as far as the development of the country’s economy is concerned. The Centre for Global Development (2015) has observed that because of high standard measures of KYC, practices of “de-risking” in which banks have distanced themselves from whole categories of higher risk clients has occurred. This has especially been the case in correspondent banking relationships, remittances, and non-profit organizations that are in high-risk areas. Analyzing these issues, one can identify that the primary concern of both, financial institutions and regulators, still stays in the question of how to provide reasonable due diligence that could protect from foreseeable risks and, at the same time, ensure financial inclusion. The problem of bringing together measures against the financing of terrorism and AML concerns with economic development considerations is central to the ongoing development of the KYC process.

To date, the KYC processes fail in identifying the beneficial ownership in such structures used in money laundering activities. Criminals use the shell companies and trusts to conceal the actual origin and ownership of unlawful funds, and, therefore, it is almost impossible for the banks to establish who is behind the transactions in question (Tupman, 2015). This challenge is however made worse by the fact that there are differences in the laws and the extent to which information is disclosed in the different jurisdictions. Nominee directors, bearer shares, and multi-layered legal entities make it even more challenging to determine who is behind these legal entities.

4.4.3. Collaboration and Information Sharing Initiatives

Furthermore, understanding the disadvantages of a number of totally separated strategies, many banks have expanded work in the framework of partnerships and joint sharing of information. As explained by the authors Maxwell and Artingstall (2017), these partnerships enable the banking industry to share information on new threats and typologies. In the future a much more dynamic responsive approach like that of the UK’s Joint Money Laundering Intelligence Taskforce (JMLIT) is somewhat more encouraging. However, their information sharing is not an outright affair since it is swindled by legal and operational issues. Croal (2008) argues that the data privacy laws can hamper the ability of banks to share their customer details for anti-crime purposes. There are also competition issues that exist, where some institutions may not want to reveal certain information or analysis that provides a competitive edge.

More important is that the idea of global information exchange is still incompletely realized. As for the regional experiences with combating financial crimes, Zetzsche et al. (2023) stipulate that effective fight against the transnational financial offenses calls for stronger cooperation with enhanced jurisdictional sovereignty that would allow for the shared preliminary intelligence.

4.5. The Role of Consulting Firms in Shaping Financial Crime Compliance Strategies

4.5.1. Development of Risk Assessment Frameworks

Consulting firms have significantly influenced the evolution of risk assessment methodologies in financial institutions. These organizations have devoted a significant amount of capital to developing complicated risk rating systems which now take into account numerous factors and contingencies (McKinsey, 2015). They allow for the optimization of specific compliance regulations and their relation to other ongoing processes within the banks. Specifically, the models created by consultancies can sometimes include machine learning and advanced analytics features that give real-time risk growing assessments and threats that are constantly appearing and constantly evolving the regulatory environment (Eceiza et al., 2020, p. 276).

Nonetheless, the overall applicability of these risk assessment instruments have been an area which is still an issue of discussion in the sphere of finance. Some critics have been saying that many frameworks further practical obscurities in that they pay as much attention to the mere compliance with the letter as to the real risk (Turkington, 2019). It may also lead institutions to channel resources to such activities whose impacts cannot be easily quantified while at the same time ignoring more substantive risks. In addition, risk assessment may be problematic at times because the use standardization may not adequately address the various risk factors that apply to various institutions, and to various jurisdictions (de Koker & Turkington, 2015).

The link between consulting firms and financial institutions regarding measures to create risk frameworks leads to possible conflict of interest. There has been controversy whether consultancies are fit to advise organizations on risk management frameworks while at the same time being in a position to sell the solutions that can help manage the risks. Such dynamics could lead to low quality and over-complicated compliance programs even when they are generating consulting revenues in the process of preventing risks, while neglecting the specific risks in question. These frameworks may also make the complexities of delivering FRAs understandable only via the intermediation of expert specialists, thus preventing the growth of knowledge about risk assessment directly in financial institutions themselves (Nestor, 2004).

4.5.2. Implementation of Technological Solutions

Consulting firms are currently right at the forefront when it comes to identifying and seeking to design and deploy technological solutions for financial crime compliance. Established professional service firms have started developing separate AI/ML/Big Data practices for AML/CFT engagements (Eceiza et al., 2020). These advanced tools are expected to help improve the speed and efficiency of numerous compliance activities such as transaction monitoring, customer due diligence and sanctions screening. The combination of those technologies is designed to perform repetitive tasks, recognize multifaceted patterns, and generate better risk assessments than tradition-based sets of rules (Maxwell & Artingstall, 2017).

Still, it is impossible to overestimate the role of technological solutions in enhancing the scale and complexity of monitoring capacities, the role of which in preventing financial crime remains ambiguous. De Koker and Turkington (2015) also note the danger of "tech-washing" in which an institution acquires seemingly impressive solutions that do not tackle key structural problems in the compliance regime. This phenomenon may in fact give an organization/companies a false sense of security and possibly dissipate resources that could otherwise be used in other areas of tackling financial crimes. Also, due to the high level of technology's development in this area there could be a constant process of refreshing the tools and applying new ones, which might be unbeneficial for institutions concerning their resources and working processes interruptions.

It is crucial to ask where accountability and/or transparency is located when tech tools become the new norm for compliance management supported by artificial intelligence. Closely related to the data situation, Guihot and McNaught (2021) raise concerns about the so-called 'black box' character of many of the machine learning algorithms applied in the systems of compliance. The fact that some of these algorithms are difficult to decode can prove to be a concern especially to regulators and institutions as they are likely to experience difficulty in determining the rationale for risk identification and management. This may also limit the compliance staff's capacity to defend and rationalize decisions resulting from interpretations by algorithms, thereby generating legal and reputational vulnerabilities for financial institutions (Zetzsche et al., 2023).

4.5.3. Training and Capacity Building

A large part of the training and capacity building responsibilities relating to the compliance function in financial institutions is provided by consulting firms. Due to expansion of statutes, rules and enforcement mechanisms, there are elaborate training programs and certification courses meant to enhance professionalism of compliance staff. These attempts at seeing that AML/CFT controls are well implemented for various establishments without compromise of organizational factors. From the consulting firms' approach to training, it is clear that practical training in the form of case studies, simulations and activities aims to fill the gap between classroom training and actual practice (Beekarry, 2011). The rationale of this approach is in the training of the compliance professionals to effectively operate in the complex environment of countering financial crime.

Although it is possible to cover a great amount of information in a training program, practical application of the newly gained knowledge in a situation where the applicant finds themselves under a considerable amount of pressure at work is usually lacking in many degrees. Johnson (2003) notes that although compliance staff may be able to learn the rules and principles, they may fail in the ability to apply them in a practical sense whenever there is conflict of business interests. This mismatch leads to the compliance function with a good framework on paper, but when executed, it does not address compliance problems as it should. Also, it is stated that the threats and challenges that are related to financial crime are changing at a fast pace along with the regulatory requirements and demands they also change frequently (Ferwerda, 2009), which may make the content of the training obsolete rapidly.

The over-reliance on external consultants could probably stifle the build-up of an internal capability between financial institutions and experts in relevant fields of study. According to Nestor (2004), such a dependence on external knowledge can be problematic for the banks since they become exposed to deficiencies in consultants, consultant mobility or shift in regulatory requirements. This is because consulting engagements are usually short-term and may not offer enough depth when it comes to the accumulation of institutional memory, which may in turn be risky to the credibility of the compliance program in the long run. Additionally, the formalization of a large number of training enabled by consultants usually are not Very sensitive to the specific risk maps and deploying contexts of each institution, again calling for the more targeted, institution – specific approaches to the capacity enhancement (Gill & Taylor, 2004).

4.6. Government Regulations and Enforcement in Combating Financial Crime

4.6.1. Evolution of Regulatory Frameworks

Bureaucracies around the globe have greatly developed and elaborated the regulative structure to prevent and punish financial crime in the course of decades. This evolution has been mainly triggered by the compliance with International requirements formulated by organizations such as Financial Action Task Force (FATF), which have been successively integrated into national laws (Alexander, 2000). The net effect has been the development of far reaching and integrated measures regarding the AML/CFT regimes across the jurisdictions. Such frameworks often cover various aspects of the measures such as the customer's due diligence measures, the reporting of suspicious transactions, and the risk-based supervision of the financial institutions. The emergence of these legal bodies has been predicated upon a rising understanding of the integration of the world's finances and the internationality of many financial offenses (Cuellar, 2002).

While there have been attempts towards harmonization of these codes and standards, the application and even the success of these regulatory models varies all across the globe. Fig 6 depicts the extent of jurisdictions' compliance with recommendations of FATF and results indicate that it is in a declining trend. The former may include elements like different legal frameworks, limited resources, as well as dissimilar degrees of commitment to combat financial crime. According to De Koker and Turkington (2015), there is an inequality in expanding on and implementing the international standards while at the same time neglecting the local risk-based approaches that best address the diverse threat environments. This is the type of tension that does not have a clear solution where global standards are necessary, but local conditions make it difficult to achieve.

The swift advancement of digitization in financial sectors and emergence of Cryptocurrency has put tremendous pressure on the existing legal framework. As Zetzsche et al. (2023) explain, traditional AML/CFT rules are developed to combat the risks inherent in identifiable traditional banking structures and thus they are not well-equipped to solve DeFi challenges or challenges posed by P2P payment systems or virtual assets. This regulatory lag makes it possible for there to be certain vulnerabilities that may be required by bad people to use in moving and also in laundering their money. As more new technologies appear, authorities and regulators are actively discussing the possible approaches to integrate the modern developments into the existing governmental and non-governmental formal theories and avoid prejudice of financial liberalization and innovation. This is due to the fact that the technological advancement in this area is ever-evolving, and thus requires a more proactive effort in the advancement of rules as a legal institution (Arner et al., 2021).

4.6.2. Enforcement Actions and Penalties

Regulatory authorities have over the years used 'high-profile' enforcement actions and heavy fines to encourage organizations to adhere to the rules against financial crime. A study done by Partnoy in 2010 shows that there has been a rise in the establishment's regulators that fine the large banks multiple billions of dollars for AML/CFT negligence especially after the credit crunch of 2008. The above actions are meant to militate against and scare off the would-be errant actors in the financial markets and bring the desired change in the sector. These penalties are indicative with regard to the dimension of the increasing acknowledgement of the systemically intricate nature of financial crimes and the supervisory function of financial institutions. Enforcement actions can also involve conditions that deal with remedial measures such as compliance program improvements, independent compliance monitoring and changes in management that seek to correct causes of failure in compliance programs (Barth et al. , 2009).

As it was mentioned earlier, the efficiency of this type of the punitive approach towards prevention of financial crime is still an object of the discussion among the academic and the policy makers. Although, there is no doubt that it has raised the importance of compliance within the financial institutions, some argue that it leads to very defensive and ineffective compliance. According to the Centre for Global Development (2015), the culture of risk aversion as a result of concern of action by the regulators has led to a common practice of de-risking where banks tend to sever business relationships with all clients or jurisdictions in the respective categories. While this kind of practice may be beneficial to the involved parties in one way or another, it also has its drawbacks that may be counterproductive to efforts aimed at promoting financial services accessibility while at the same time possibly shifting some transactions to less regulated channels. Also, emphasis on the huge fines will mislead the regulators from other major aspects of fighting financial crimes for instance in the collection of intelligence and risk prevention (de Koker & Turkington, 2015).

Scrutiny is being felt on the fact that large fines may be easily perceived by some big financial institutions as the set cost of operation instead of giving the required significant shift in corporate culture. According to Levi (1991), it is argued that given that large banks can afford to take heavy penalties, their deterrent effect may be off-set. This dynamic brings into question the efficacy of monetary sanctions in the long run, in modifying institutional behavior. At the same time, smaller institutions may be exposed to higher existential risks in case of compliance violations which will only worsen the issue of an uneven racial playing field in the financial sector. There are other approaches where some argue that there should be a harmonized style of enforcement that includes financial measures and structural reforms along with the individual measures, and a possible reward system for good compliance programs (Beekarry 2011).

4.6.3. Public-Private Partnerships and Information Sharing

As most countries are now aware of the inability of conventional forms of laws to address the problems of financial crimes, governments have invited private organizations to join their efforts in fighting financial crimes. Other measures such as the UK's Joint Money Laundering Intelligence Taskforce (JMLIT) involves representatives of police, the regulating authorities and financial sectors in sharing the intelligence and centralizing efforts in combating new trends. These collaborative models shall try and capitalize on the strengths of both the public and private sector. In this regard, through the provision of real-time information sharing and collaborative analysis, such partnerships may help to ensure that financial crime prevention is a more timely and reflexive process. Similar programmed have been implemented in other jurisdictions thus demonstrating that a shift toward more partnership and intelligence approaches is becoming more common in the fight against financial crime (Eceiza et al., 2020).

There is much hope towards these PPP especially towards the area of improving and expanding infrastructure, however the questions appear in relation to matters such as privacy of data and information, competition and distinguishing between public and private spheres. Croal (2008) observes that data protection laws also put limitations on the sharing of customers' information by the financial institutions, including for the fight against crime. Preserving communication on the one hand while respecting privacy and civil liberties on the other is however a challenge that has not yet been met appropriately. Also, there is a fear of capture and possible conflicts of interest given that some of the private sector individuals and institutions become key players in the formulation of enforcement goals and objectives. Some of the factors worth considering while designing and executing these frameworks include; precaution to ensure participants on all sides of the collaboration equally get access to raw information; to avoid the abuse of the provided information; and to check on the accountability of all the participants more so the intelligence gleaned from the common platform (Guihot & McNaught, 2021).

However, as positive as these regional reports may be, and as effective as they may be therefore, there continues to be no global coordination in fighting financial crime. According to the Financial Stability Board (2020), in order to be effective in dealing with transnational financial crimes, more stringent structures of international cooperation should be developed, capable of withstanding the differences in the legal systems of different nations whilst allowing for cooperation in the collection of intelligence and practical actions. They include issues related to legal systems, definitions of predicate offenses and political considerations with regard to the exchange of information across borders. Changing international financial environment, as well as the development of new means of financial crimes, such as those involving cyber-space, also points to the importance of improved cooperation across state borders. Efforts to establish territorialized measures for the activation of global coordination mechanisms, including changes in roles of the international organizations or creation of the new multilateral treaties, are still continued, though political and practical obstacles are rather essential (Zetzsche et al. , 2023).

5. Conclusion

In conclusion, this systematic review has analyzed the alteration of financial criminality in contemporary society due to advanced technology as well as the possibility of cooperation between Banks, Consultancy firms and Governments for enhanced fight against this kind of criminality. The issues of research concerns are as follows; the sophistication of the financial crimes, the failure of the compliance models, and the magnitude of IFFs which according to UNODC (2011) ranges between $2 trillion and $5 trillion annually. Thus, the digital finance platforms coupled with the cryptocurrencies amplify the work of trying to identify and prevent those financial crimes while narrowing down the methods that may not work as effectively as the new paradigms of technology would require.

The study also stresses that cooperative approaches and public-private partnerships can be effective in managing them. In this paper, Zetzsche et al. (2023) describe the elements of what the authors called the trifecta approach, which can use the comparative advantages of a bank, a consulting firm, and a government to ensure more efficient prevention of financial crimes. Though, use of such approaches of collaboration presuppose the functions of the regulation together with the need to spur innovation and achieve objectives in financial inclusion. Their research also clearly underlines the importance of the global cooperation and the setting of common rules and standards to fight the executive offenders in cross-border financial crimes, and the importance of the adequate working of those international standards on all the levels of the affected countries.

Emerging technologies for example big data, biometrics, artificial intelligence, ML, cloud computing, blockchain etc have great potential of increasing effectiveness in financial crimes control. New technologies may provide better means for identifying suspicious behaviors, better measures for assessing risks, and timely identification of threat. But, it has been observed that their use also poses significant ethical, legal and governance questions which have to be resolved.

5.1. Future Research

Hence, the continuously growing dynamic complexity of financial crimes in the digital age entails many opportunities for future research. These models and partnerships demand additional examination especially in how sustainable they are in the fight against financial crime. Longitudinal could be used to measure the effectiveness of these initiatives in relation to detection, prevention and financial system integrity. Subsequently, the studies focused on the possible tradeoffs between the required regulatory measures, technological advancements and access to money services businesses in different places and countries.

One of the other crucial topics that requires further investigation in the future is the use of modern technologies in countering financial crimes. Certificates such as data analytics, or machine learning, or blockchain have been identified but there is a need for quantitative analysis for their efficiency and effectiveness as well as the guidelines for their implementation. This could be in the form of a comparison of various technological solutions and their performances as well as the impact of the results in different banks and within different legal contexts.

How some of these new financial technologies such as the FinTech and the DeFi are influencing the kind and incidence of financial crimes as well as measures put in place is another promising research direction for the future. Future research may analyze how these new financial landscapes transform the types of financial crimes and the difficulties that old-fashioned legal and law enforcement mechanisms present. These findings could be of significant use in the creation of new regulatory models and measures to fight the youth of these novel financial systems. In addition, literature from the fields of finance, law, computer science and behavioral economics likely contains frameworks that might offer useful insights into the nature of financial crime within digital environments. Research of this type of work could look at identification of psychological and sociological factors that prompt the performance of financially related crime in digital environments and the ways knowledge of these aspects may facilitate improved financial crime prevention.

Recommendations

Based on the findings of this study, several key recommendations can be made to enhance the effectiveness of financial crime prevention efforts in the digital era: Based on the findings of this study, several key recommendations can be made to enhance the effectiveness of financial crime prevention efforts in the digital era:

- **Foster Collaborative Approaches:** It is here that various links of the chain and industry players such as the financial institutions, regulatory bodies, and technology providers should embrace and contribute to collaborative efforts or public private partnership. These partnerships should entail exchange of information, ideas and technological tools that would enhance synergism in the fight against financial crime.
- **Invest in Advanced Technologies:** There is a need for financial institutions and regulatory bodies to invest in areas such as big data analysis, artificial intelligence and Distributed Ledger Technology (blockchain). All these technologies hold the promise of strengthening the fight against the commission of financial crimes, but their application must come hand in hand with proper governance structures whose lacking often leads to problems such as violation of data privacy or algorithmic bias.
- **Adopt Risk-Based Approaches:** From the current generalized approach to combating financial crime, regulators and financial institutions should shift to risk-based approaches. This shift may assist in the optimization of the crime prevention objectives with the objectives of financial sector development and innovation. To address it, we need to design better risk assessment frameworks that would be more relevant in the context of the fight against financial crime at a time when it is being increasingly shifted to digital platforms.
- **Enhance International Coordination:** Most of the financial crimes are transnational in nature which requires increased drive in the issuing of standards and enforcement at the international level. Overarching, global approaches should be promoted by the international organizations in the area of financial crime with an aim to develop more responsive and standard-rooted solutions, which can however be coupled with the provision of resolution processes for the matters specific for certain jurisdictions.
- **Prioritize Financial Inclusion:** Financial crime prevention strategies therefore require stakeholders to comprehensively factor in financial inclusion when charting their financial crime prevention strategies. Some care should be taken to avoid some negative side effects, such as de-risking that has the effect of locking out many genuine clients and operations from the formal economic system.
- **Invest in Capacity Building:** This means that there should be a massive commitment to investments towards capacity building especially in the emerging markets so that all the jurisdictions are well equipped to fight financial crime. This comprises indoctrination in new technologies and techniques, and assistance in putting in place sound legal requirements.
- **Promote Regulatory Innovation:** It is argued that regulators should consider the utilization of methods like the regulatory sandboxes to permit the trial of new technologies or otherwise in financial crime mitigation. From this, it will be possible to enhance innovation while at the same time, managing the risks which are involved appropriately.

Thus, the implementation of the provided recommendations will help the stakeholders to develop a better viable English system to fight with financial crime in the globally more and more complicated and technologically advanced environment.

References

[1] Alexander, K. (2000). The Role of Soft Law in the Legalization of International Banking Supervision: A Conceptual Approach. ESRC Centre for Business Research, Cambridge University, Working Paper 168.

[2] Alliance for Financial Inclusion. (2022). Inclusive Green Finance. https://www.afi-global.org/thematic-areas/inclusive-green-finance

[3] Arner, D., Buckley, R., Zetzsche, D., Didenko, A., Zhao, L., & Andhov, M. (2021). A principles-based approach to the governance of BigFintechs. United Nations Development Programme. https://www.undp.org/sites/g/files/zskgke326/files/2021-10/UNDP-UNCDF-TP-3-3-A-Principles-based-Approach-to-the-Governance-of-BigFintechs-EN.pdf

[4] Baltensperger, E., & Dermine, J. (1987). The role of public policy in ensuring financial stability. In R. Portes & A. Swoboda (Eds.), Threats to International Financial Stability. Cambridge University Press.

[5] Barth, J. R., Gan, J., & Nolle, D. E. (2009). Global Banking Regulation and Supervision. Nova Science Publishers.

[6] Becker, G. S. (1968). Crime and Punishment: An Economic Approach. Journal of Political Economy, 76(2), 169-217.

[7] Beekarry, N. (2011). The International Anti-Money Laundering and Combating the Financing of Terrorism Regulatory Strategy: A Critical Analysis of Compliance Determinants in International Law. Northwestern Journal of International Law and Business, 31, 137-193.

[8] Bhagat, S. (2022, March 31). An inconvenient truth about ESG investing. Harvard Business Review. https://hbr.org/2022/03/an-inconvenient-truth-about-esg-investing

[9] Boffo, R., & Patalano, R. (2021). ESG investing: Practices, progress and challenges. OECD. https://www.oecd.org/finance/ESG-Investing-Practices-Progress-Challenges.pdf

[10] Bosworth-Davies, R., & Saltmarsh, G. (1994). Money Laundering: A Practical Guide to the New Legislation. Chapman and Hall.

[11] Busuioc, E. M. (2007). Defining Money Laundering. In B. Unger, The Scale and Impacts of Money Laundering. Edward Elgar.

[12] Carrière-Swallow, Y., Haksar, V., & Patnam, M. (2021). India's approach to open banking: Some implications for financial inclusion (IMF Working Paper WP/21/52). International Monetary Fund.

[13] Centre for Global Development. (2015). Unintended Consequences for Anti-Money Laundering Policies for Poor Countries. CGD Working Paper.

[14] Civils daily, (2020) Public Private Partnership Models: Contracting, Build Operate Transfer, Design Build Finance Operate (DBFO), Concessions, Build Operate Transfer, EPC Model, Swiss Challenge Model, HAM [online]available from https://www.civilsdaily.com/public-private-partnership-models-contracting-build-operate-transfer-design-build-finance-operate-dbfo-concessions-build-operate-transfer-epc-model-swiss-challenge-model-ham-model/ .

[15] Clarke, M. (1995). What Is Compliance? The Moral Dimension. Journal of Financial Regulation and Compliance, 3(2), 123-134.

[16] CoinGecko. (n.d.). CoinGecko [Website]. https://www.coingecko.com

[17] Council of Europe. (1980). Measures Against the Transfer and Safekeeping of Funds of Criminal Origin, R (80) 10.

[18] Croal, H. (2008). Combating financial crime: regulatory versus crime control approaches. Journal of Financial Crime, 11(1), 45-55.

[19] Cuellar, M. F. (2002). The Tenuous Relationship Between The Fight Against Money Laundering And The Disruption Of Criminal Finance. Journal of Criminal Law And Criminology, 93(2-3), 311-466.

[20] de Koker, L., & Turkington, M. (2015). Anti-money laundering measures and the effectiveness question. In B. Rider (Ed.), Research Handbook on International Financial Crime (pp. 520-535). Edward Elgar.

[21] DeFi Pulse. (2021). DeFi Pulse [Website]. https://defipulse.com

[22] Eceiza, J., Kristensen, I., Krivin, D., Samandari, H., & White, O. (2020). The future of operational-risk management in financial services. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-future-of-operational-risk-management-in-financial-services

[23] European Economic Community. (1991). On prevention of the use of the financial system for the purpose of money laundering, COUNCIL DIRECTIVE (91/308/EEC).

[24] Evans, P. C., & Gawer, A. (2016). The rise of the platform enterprise: A global survey. The Center for Global Enterprise. https://www.thecge.net/app/uploads/2016/01/PDF-WEB-Platform-Survey_01_12.pdf

[25] Favarel-Garrigues, G. (2005). Domestic reformulation of the moral issues at stake in the drive against money laundering: the case of Russia. International Social Science Journal, 185, 529-541.

[26] Ferwerda, J. (2009). The Economics of Crime and Money Laundering: Does Anti-Money Laundering Policy Reduce Crime? Review Of Law and Economics, 5(2), 903-929.

[27] Financial Stability Board. (2020). BigTech firms in finance in emerging market and developing economies: Market developments and potential financial stability implications. https://www.fsb.org/wp-content/uploads/P121020-1.pdf

[28] Flugum, R., & Souther, M. E. (2022, September 13). Stakeholder value: A convenient excuse for underperforming managers? Social Science Research Network. https://ssrn.com/abstract=3725828

[29] Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., & Zbinden, P. (2019). BigTech and the changing structure of financial intermediation (BIS Working Papers No. 779). Bank for International Settlements. https://www.bis.org/publ/work779.htm

[30] Gill, M., & Taylor, G. (2004). Preventing Money Laundering or Obstructing Business? Financial Companies' Perspectives on "Know Your Customer" Procedures. British Journal of Criminology, 44, 582-594.

[31] Goodhart, C. (2011). The Basel Committee on Banking Supervision: A History of the Early Years, 1974-1997. Cambridge University Press.

[32] Guihot, M., & McNaught, H. (2021). Platform power, technology, and law: Consumer powerlessness in informational capitalism. Law, Innovation and Technology, 13(2), 510-534.

[33] Haberly, D., MacDonald-Korth, D., Urban, M., & Wójcik, D. (2019). Asset management as a digital platform industry: A global financial network perspective. Geoforum, 106, 167-181.

[34] Henderson, R., & Walker, O. (2022, February 26). Inside BlackRock's black box: The world's most powerful risk management system threatens to become a liability for its owner. Australian Financial Review. https://www.afr.com/companies/financial-services/does-blackrock-s-aladdin-have-too-many-under-its-spell-20200226-p544ex

[35] Hodgson, D. (1984). Profits of Crime and Their Recovery. Howard League for Penal Reform.

[36] Hornuf, L., Klus, M. F., Lohwasser, T. S., & Schwienbacher, A. (2018). How do banks interact with fintechs? Forms of alliances and their impact on bank value. CESifo Working Paper Series No. 7170.

[37] https://www.econstor.eu/handle/10419/264403

[38] IMF, Implementation of Governance Measures in Pandemic-Related Spending (July 2023). https://www.imf.org/-/media/Files/Topics/governance-and-anti-corruption/implementation-of-governance-measures-in-pandemic-related-spending-july-2023.ashx

[39] International Monetary Fund Staff. (n.d.). IMF Data [Website]. International Monetary Fund. https://www.imf.org/en/Data

[40] Jain, S. (2022, September 13). The G20 digital economy agenda for India. Observer Research Foundation. https://www.orfonline.org/wp-content/uploads/2022/09/ORF_OP-365_India-G20-Digital-Economy.pdf

[41] Jenkins, I. (2018, February 23). Collaboration not competition: Banks find new partners. PWC. http://pwc.blogs.com/fintech/2016/08/banks-collaboratewith-fintechs-rather-than-viewing-them-as-competition.html

[42] Johnson, J. (2003). How will the financial sector respond to the Financial Action Task Force's increased customer due diligence requirements? Journal of International Banking Regulation, 5(2), 127-145.

[43] Klapper, L., Lusardi, A., & Van Oudheusden, P. (2015). Financial literacy around the world. Global Financial Literacy Excellence Center. https://gflec.org/wp-content/uploads/2015/11/Finlit_paper_16_F2_singles.pdf

[44] Klus, M. F., Lohwasser, T. S., Holotiuk, F., & Moormann, J. (2019). Strategic alliances between banks and fintechs for digital innovation: Motives to collaborate and types of interaction. The Journal of Entrepreneurial Finance (JEF), 21(1), 1-23.

[45] Levi, M. (1991). Regulating Money Laundering: The Death of Bank Secrecy in the UK. The British Journal of Criminology, 31(2), 109-125.

[46] Lontchi, C. B., Yang, B., & Su, Y. (2022). The mediating effect of financial literacy and the moderating role of social capital in the relationship between financial inclusion and sustainable development in Cameroon. Sustainability, 14(23), 15093.

[47] Lord Turner. (2009). The Turner Review: A regulatory response to the global banking crisis. Financial Services Authority.

[48] Maxwell, N., & Artingstall, D. (2017). The Role of Financial Information-Sharing Partnerships in the Disruption of Crime. Royal United Services Institute (RUSI).

[49] McKinsey and Company. (2015). The future of bank risk management. McKinsey & Co. Risk Work Paper.

[50] Merton, R. C. (1995). Financial innovation and the management and regulation of financial institutions. Journal of Banking & Finance, 19(3-4), 461-481.

[51] Nestor, S. (2004). The impact of changing corporate governance norms on economic crime. Journal of Financial Crime, 11(4), 347-352.

[52] Onyango, S. (2022, May 4). Africa accounts for 70% of the world's $1 trillion mobile money market. Quartz Africa. https://qz.com/africa/2161960/gsma-70-percent-of-the-worlds-1-trillion-mobile-money-market-is-in-africa

[53] Partnoy, F. (2010). Infectious Greed: How deceit and risk corrupted the Financial Markets. Profile Books. https://books.google.com/books?hl=en&lr=&id=-Gno2HUfBLUC&oi=fnd&pg=PR13&dq=The+Trifecta+Against+Financial+Crime&ots=_BPbrEdnXo&sig=xs5oSDFXKaIJT1aQ3hzKLBSsgtk

[54] Perlman, R. (2021, May 11). EU's Sustainable Finance Action Plan takes shape: New proposals for climate reporting and green investments. Herbert Smith Freehills. https://www.herbertsmithfreehills.com/insight/eus-sustainable-finance-action-plan-takes-shape-new-proposals-for-climate-reporting-and

[55] S&P Global Market Intelligence. (2012). About Us. S&P Global. https://www.spglobal.com/marketintelligence

[56] Tupman, W. (2015). The characteristics of economic crime and criminals. In B. Rider (Ed.), Research Handbook on International Financial Crime. Edward Elgar.

[57] Turkington, M. (2019). The effectiveness of private sector engagement in international financial crime countermeasures (Doctoral dissertation, La Trobe).

[58] United Nations Educational, Scientific and Cultural Organisation. (2018, June). A global framework of reference on digital literacy skills for Indicator 4.4.2 (Information Paper No. 51,

[59] Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2023). Sustainability, Financial Inclusion and Efficiency: A Trilemma or a Trifecta for the Regulation of Digital Finance? Banking & Finance Law Review, Forthcoming. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4527464