# Anti-money laundering and customer due diligence: empirical evidence from South Africa

William Gaviyau and Athenia Bongani Sibindi
*Department of Finance, Risk Management and Banking, College of Economic and Management Sciences, University of South Africa, Pretoria, South Africa*

## Abstract

**Purpose** – The purpose of this study is to examine the South African banks' customer due diligence (CDD) practices in the fintech era to mitigate money laundering (ML) risks and ensure financial stability. Financial technologies have brought substantial transformations to the financial services sector. However, such technologies have exposed the sector to emerging risks that threaten the integrity and stability of the financial system globally. Before any bank–customer relationship is established, proper customer background checks must be conducted. These background checks enable financial institutions to validate information provided and ensure customers are properly risk profiled. Failure to risk profile customers could result in financial institutions being used as conduits for ML. Undoubtedly, CDD procedures are pivotal to overall anti-money laundering efforts and curbing financing terrorism in a regulatory framework.

**Design/methodology/approach** – A qualitative research approach was adopted to address the research questions of the study. Given the confidentiality associated with the financial services sector, data triangulation was used in blending mainly secondary and primary data sources. Secondary data sources used in the study were published reports available in the public domain that were corroborated with subject matter experts' interviews.

**Findings** – Based on the findings of this study, it is concluded that in South Africa, technological solutions have been incorporated into CDD functions, which is now risk-based (enhanced due diligence). Also, legally, South Africa has incorporated the biometrics, integration with Department of Home Affairs and Companies and Intellectual Property Commission databases, customer consent to third-party sources with the Financial Intelligence Centre Act and the Protection of Personal Information Act.

**Originality/value** – The shift towards digital banking in South Africa results in increased data and dynamic risk profiling. This study advocates a policy shift requiring a risk-based approach to mitigating emerging ML risks (in particular digital laundering), especially in the wake of South Africa's recent greylisting by the Financial Action Task Force.

**Keywords** Terrorism, Money laundering, Financial Action Task Force, Customer due diligence, Digital banking, Enhanced due diligence, Greylisting, Third-party vendor systems

**Paper type** Research paper

## 1. Introduction

Effective customer due diligence (CDD) procedures are integral to fighting money laundering (ML) and associated risks (Sunarmi *et al.*, 2022; Johari *et al.*, 2020; Trajkovski and



*Funding*: The Article Processing Charges were funded by the University of South Africa.

Journal of Money Laundering Control
Vol. 26 No. 7, 2023
pp. 224-238
Emerald Publishing Limited
1368-5201
DOI 10.1108/JMLC-06-2023-0103

Nanevski, 2019; Raweh *et al.*, 2017). This is a proactive stance adopted against these ever-increasing risks. The procedures for CDD entail risk profiling of customers based on verified and authenticated customer documents prior to establishing a bank–customer relationship. Failure to conduct appropriate customer risk profiles during periodic reviews and onboarding could result in financial institutions being conduits for ML (Sultan and Mohameed, 2022; Cindori and Petrovic, 2018; Esoimeme, 2015). Accordingly, the International Monetary Fund (IMF) (2015) argued that fighting ML is a complex process which demands extensive resources. Furthermore, Harry and Suntura (2020) suggested that the creation of strong and robust customer identification systems is the greatest challenge in the anti-money laundering (AML) architecture.

Consequently, in the era of digital innovations, banks need to relentlessly update their risk and compliance management programmes. However, the AML framework stresses the need to exercise caution in dealing with innovative technologies. Failure leaves financial institutions with AML and combatting of financing terrorism (CFT) technologies that lag behind risk compliance systems and at the mercy of regulators. Technological innovations have forced the financial services sector to adopt digital banking platforms, rely on third-party shared services to perform regulatory process, adopt risk-based AML/CFT approaches and use analytics (Gaviyau and Sibindi, 2023; Matsuo and Staines, 2020; Phanwichit, 2018).

Globally, AML/CFT efforts are enhanced by the Financial Action Task Force (FATF). These efforts are aimed at expanding the resilience of financial institutions in curbing ML and the concomitant financing of terrorism. The FATF is an organisation under the auspices of the Organisation for Economic Co-operation and Development that specialises in combatting ML (FATF, 2012). It has set minimum criteria known as the 40 recommendations for combatting ML (Chitimira and Munedzi, 2022; Sujee, 2016).

The countries' AML/CFT regulations to which financial institutions adhere are drawn from the FATF recommendations. The current research is underpinned by FATF Recommendations 10 and 15. FATF Recommendation 10 specifies the need for CDD, while FATF Recommendation 15 deals with financial institutions being cognisant of threats arising from new or developing technologies that enhance anonymity (FATF, 2018). The CDD measures (identification, verification, nature of business relationship and ongoing monitoring) need to be enforced rigorously. Given increased regulatory oversight after the 2007/2008 global financial crisis (GFC), failure to comply with AML/CFT regulations results in regulatory risk both at the institution level and the country level.

In line with the FATF recommendations, South Africa passed several pieces of legislation to deal with ML and the financing of terrorism. These include Prevention of Organised Crime Act (POCA, Act No. 121 of 1998) and the Financial Intelligence Centre Act (FICA, Act No. 38 of 2001) among others. All these pieces of legislation are interlinked to ensure that no legal loopholes exist (Chitimira and Munedzi, 2021; Sujee, 2016). FICA and POCA are closely interlinked.

Periodic country mutual evaluations are conducted by the FATF. Comparing the 2009 and 2021 mutual evaluation reports, South Africa progressively made concerted efforts to ensure compliance with the 40 FATF recommendations. Clearly, the existence of a legal framework does not guarantee its effectiveness or adequacy (Mniwasa, 2019; Maguchu, 2018; Sujee, 2016).

Before any bank–customer relationship is established, proper customer background checks need to be conducted (Chitimira and Munedzi, 2022; Osifo, 2020; Viritha and Mariappan, 2013; FATF, 2012). These background checks enable financial institutions to validate information provided and ensure that clients are properly risk profiled (Sultan and Mohameed, 2022). Failure to risk profile customers results in financial institutions being

used as conduits for ML (Beebeejaun and Lubnaa, 2022; Cindori and Petrovic, 2018; Esoimeme, 2015). Undoubtedly, CDD procedures are pivotal to the overall AML/CFT regulatory framework (Fulop *et al.*, 2022; Johari *et al.*, 2020; Trajkovski and Nanevski, 2019; Raweh *et al.*, 2017).

Against this background, the aim of this study was to examine the South African banks' CDD practices in the fintech era to mitigate ML risks and ensure financial stability. Based on this aim, the four objectives of the study were as follows:

(1) to assess the South African banks' individual customer identification and verification practices in the fintech era;

(2) to determine the South African bank customer's nature and the purpose of business relationship practices of CDD in the fintech era;

(3) to examine the South African bank customer's ongoing due diligence measures applied in the fintech era; and

(4) to evaluate the AML/CFT regulatory enforcement actions effected on South African banks in the fintech era.

The rest of the article is organised as follows: Section 2 reviews the related literature. The research methodology applied in the study is described in Section 3. The empirical findings are presented and discussed in Section 4, and Section 5 concludes the article.

## 2. Review of related literature

This section outlines the related literature on the theories, CDD measures and AML/CFT regulatory enforcements.

### *2.1 Theoretical literature review*

When integrated, ML and information and communications technology adoption theories can explain the behaviour of financial sector players in responding to the fintech developments of mitigating emerging ML risks.

#### *2.1.1 Money laundering theories*

2.1.1.1 Crying wolf theory. The crying wolf theory was advanced by Takats (2007) to explain the enforcement of AML regulations by bank regulators. This theory intimates that an agency relationship exists between banks and the government or customers. These relationships are associated with information asymmetries. The crying wolf theory is based on five economic building blocks: information, reporting, fines, monitoring and investigations. Gara and Pauselli (2020) tested the theory empirically relative to Italian banks and confirmed its usefulness in instituting better strategies for onsite and offsite AML/CFT regulatory assessments.

2.1.1.2 Transparency stability theory. Tadesse (2006) advanced the transparency stability theory from the general disclosure regulation theory (Healy and Palepu, 2001). The behaviour of financial institutions is considerably regulated and important to economic participants (Kundid and Rogosic, 2012). Hence, the information asymmetry concept serves as the basis of the transparency stability theory. Financial information available to economic participants must be credible, useful and timely (Juntunen and Teittinen, 2022; Bushman, 2016; Eusepi, 2004). In fulfilling their regulatory mandate, regulators and the regulated need to circulate reliable financial information (Isolauri and Ameer, 2022; Bouvatier, 2014). Information disclosure and publication by regulators and financial institutions alike are considered a public good obtainable free of charge (Clarke, 2021;

Kundid and Rogosic, 2012; Watts and Zimmerman, 1986). In short, these reports should be available regularly for economic participants to make informed decisions.

2.1.1.3 Anti-money laundering systems theory. Demetis (2010) advanced the AML system theory as a panacea for understanding and explaining the AML phenomenon. Demetis (2010), as supported by Kavuni and Milne (2019), argued that to understand ML requires an interdisciplinary approach. According to the systems theory, the AML domain consists of systems and sub-systems. The AML system is broken down into three elements: transnational, national and local. These help in identifying the global AML/CFT regulatory framework. In addition, the sub-system consists of political, legal and economic spheres. Cash (2020) contended that the failure to understand that ML arises from the systematic nature of the AML/CFT framework. The resulting AML/CFT inefficiencies have been attributed to a lack of shared goals within the system.

2.1.1.4 Evolution game theory. Araujo (2010) modified the game theory, resulting in the evolutionary game theory. Modified factors that were incorporated include the regulatory framework design, organisations, employees and AML-related costs. The ML phenomenon is viewed as a game between organisations and employees (Cash, 2020). Key to this theoretical construct is the collaborative effort of regulators, banks and employees in the face of associated ML regulation challenges (Martínez-Sánchez *et al.*, 2022; Araujo, 2009a, 2009b; Masciandaro, 1999). The theory further identified that despite the critical factor of collaborative effort in fighting ML, it is endogenously affected by workers' willingness and regulatory design (Masciandaro, 1999). Hence, proper design of regulatory systems influences the effectiveness of combatting ML.

*2.1.2 Information and communications technology adoption theories*

2.1.2.1 Diffusion of innovation theory. The diffusion of innovation (DoI) theory was initially advanced by Rogers (1962) as a five-stage model for organisations implementing and adopting innovative technologies. Rogers (1962) postulated that diffusion is a process in which adopted innovation must be communicated across social networks over a period. DoI happens through a series of technology introduction, learning and adaption. It becomes successful after the benefits have been realised, with organisational effectiveness improving as well (Rogers, 1962). Lai (2017) noted that DoI is premised on establishing the foundation for conducting research on innovation, adoption and acceptance. Thus, innovation and adoption happen after sequential stages, leading to the development of an S-shaped adoption curve.

2.1.2.2 Technology acceptance model hype cycle. The technology acceptance model (TAM) combined with the hype cycle help to provide an understanding of the effect of digital innovations in the AML/CFT sphere over a period. The hype cycle was advanced by Gartner in 2007 to explain people's reactions to new technologies over time (Fennie, 2010). The TAM's proponent was Davis, in 1986, showing the process whereby users come to accept and use technology or an information system. The integration of these two models was advanced by Betts-LaCroix (2010). It shows the different levels of technology acceptance by stakeholders over a time period. Furthermore, stakeholder's technology expectations are non-linear and they exist in the form of a cycle (Shuler, 2012). The stakeholders include consumers, regulators, supervisors, the government, financial institutions, non-financial institutions, fintech firms and investors.

*2.2 Customer due diligence measures*

The CDD measures are shown in Table 1. First, customer identification and verification is discussed.

*2.2.1 Customer identification and verification practices.* Verifying and validating customer records during onboarding or on an ongoing basis is fundamental to the promotion of market integrity (Jayasekara, 2021; Gomber *et al.*, 2017; Bamberger, 2016). This ultimately prevents criminal intention in the financial system by minimising market behaviour and manipulation. The presence of AML/CFT legislation limits access to financial services, requiring balanced regulator mandates of financial inclusion, economic growth and market integrity. However, Gleb (2016) argued that to attain the market integrity objective, financial institutions need to know the type of customers they are dealing with. However, appropriate CDD rules and procedures are crucial for financial integrity and inclusion.

Findings on the developed countries confirm the application of technological innovations in performing CDD procedures. The incorporation includes the adoption of biometrics to verify and authenticate customer details, the adoption of remote customer onboarding and the use of blockchain technology to perform some CDD procedures. Countries such as Hong Kong, Estonia and other European countries have incorporated biometrics, transaction systems and remote onboarding in performing CDD procedures. Despite this progress, the issues of universal identity cards, privacy and credibility remain a hurdle or challenge. Even though financial institutions can rely on third parties or intermediaries to perform any CDD measures, the ultimate responsibility rests with the financial institution (Sharif *et al.*, 2022; FATF, 2012).

*2.2.2 Nature and purpose business relationship.* The nature of the business relationship is determined by assessing the following customer documents: source of income, type of business, financial statements, proof of residence, employment details, nationality, ownership and control structure, expected transaction volumes and expected transaction countries for inward and outward funds flow (FATF, 2018; Viritha and Mariappan, 2013). Business relationships can be established through proxies (Juntunen and Teittinen, 2022; Demetriades and Rousseau, 2016). The identification and verification of principal and proxy are needed to comply with the CDD requirements. The FATF (2014) pointed out that money launderers disguise organisations' ownership structures.

In terms of the control structure, institutions have the flexibility to find beneficial owners in charge of controlling based on the institution's risk assessment. The Companies Act in Hong Kong was amended to include information on ownership and control (Yim and Lee, 2018). This was enacted in 2017, and the amendment requires that companies have significant controllers' registers. This has to be availed upon demand by regulators (Trajkovski and Nanevski, 2019). In Germany, the *Handelsregister* electronic database for companies contains information about ownership and control structures of companies operating in that country (Christie, 2018). Banks can verify the customer information submitted against that register at a small fee.

| CDD procedures | Expectations |
|---|---|
| Identification and verification | Customer identification documents; registration documents; proof of address; contact details |
| Nature of business relationship | Employment details; source of income; expected volume of transactions; transaction geography |
| Ongoing due diligence/monitoring | Documents resubmitted; politically exposed persons; media and criminal checks |

**Source:** Researchers' own compilation

**Table 1.**
Summary of CDD procedures

*2.3 Ongoing due diligence*

Information collected for CDD requirements needs to be updated frequently. The frequency of updating a customer profile should be in line with the financial institution's customer acceptance and ML risk policy (Cindori and Petrovic, 2018; Viritha and Mariappan, 2013). Undoubtedly, the categorisation of customers helps financial institutions to monitor account transactions and activities (Mniwasa, 2019; Christie, 2018; Ferwerda, 2009). In this regard, proper risk profiling should be done first.

Customers classified as politically exposed persons (PEP) must be monitored, as they are considered high-risk clients (Bethelihem, 2019; Arasa and Ottichilo, 2015). During customer risk profiling, these are usually classified as high risk due to the nature and difficulties in identifying the owners and authentication of funds. PEP identification in United Arab Emirates using commercial databases has proved to be neither accurate nor reliable (ElYacoubi, 2020). Bethelihem (2019) confirmed that in Ethiopia, the banks had no lists of PEPs. Thus, it is possible that PEPs operate banks accounts without being identified. Therefore, banks must conduct proper background checks using independent sources to establish PEP linkages and political connections (ElYacoubi, 2020).

For completeness and reliability, other sources are needed to complement the name screening process, such as media articles and internet searches. Due care should be exercised when banking institutions rely on third parties (refer to FATF Recommendation 17). After commencement of the bank–customer relationship, the status can change and the risk profile must be adjusted accordingly (Zetzsche *et al.*, 2019). Hence, institutions ought to be alert to public information which could change customer's risk profile.

Ongoing account monitoring assists financial institutions in making informed decisions. Informed decisions are based on potential ML and terrorism financing (ML/TF) risk exposure and on subsequent risk management (Matsuo and Staines, 2020). Due to large data sets of customers' digital transactions in the modern world, regulators and financial institutions rely heavily on reporting systems to detect unusual behaviour (Oztas *et al.*, 2022). The detection mechanisms trigger enforcement and investigation. Viritha *et al.* (2015) argued that determining suspicious transactions is subjective and qualitative in nature, as this depends on the employee's judgment and logic. This justifies the need for technology-driven solutions. Existing ongoing monitoring can only be effective if CDD measures are properly followed despite the challenges.

*2.4 Anti-money laundering/combatting of financing terrorism regulatory enforcement*

Regulators use formal and informal enforcements to deter corrupt behaviour. Enforcement action is dependent on the magnitude of non-compliance. When the non-compliance is more severe, this must be formalised, publicised and prescribed legally. The safety and soundness of the financial system are affected by AML/CFT non-compliance. Various enforcements issued: cease and desist orders, forfeiture orders and monetary penalties. After the 2007/2008 GFC, much emphasis has been placed on effecting regulatory sanctions for non-compliance with the overall aim of safeguarding the financial system and improving transparency (Zetzsche *et al.*, 2019; Butler and Brooks, 2018). AML/CFT weaknesses affect the financial system's integrity and national security (Teichmann and Wittmann, 2022; Cutter, 2018).

## 3. Research methodology

Schoonenboom and Johnson (2017) defined the population as the subjects of interest in a study. The South African banks served as the target population of this study. According to the South Africa Reserve Bank (SARB, 2022), 34 registered banks are operating in the country's financial services sector. The financial sector is further categorised based on

control structure and size. The large banks control 89% of the total banking assets in South Africa. In terms of ML/TF risk, South Africa's banking sector has an inherently high ML/TF risk.

Based on the qualitative nature of the study, the case study was identified as the most appropriate, with South Africa being the case. The study's target population was South Africa's banking sector, with the respondents being AML/CFT experts. Neuman (2005) asserted that purposive sampling is useful in case study situations with small samples that need in-depth information about the subject matter. Given the confidentiality and sensitive information associated with the study, purposive sampling was applied in selecting the ten AML/CFT experts by using LinkedIn profiles. Their average AML/CFT experience was 7.9 years. This approach of using experts enables the gathering of technical information that cannot be provided by the secondary data.

As shown in Table 2, to attain the research objectives (ROs), data was obtained from secondary and primary sources. These objectives were underpinned by FATF Recommendations 10 and 15. Nevertheless, analysing the data without getting a rich understanding of the why means that the study will be inconclusive. Hence, interviews were developed to corroborate findings from the secondary data. This resonates with Teddlie and Tashakkori (2010), who asserted that answering the why question provides rich details of the phenomenon under study.

## 4. Empirical results and discussion

### *4.1 Descriptive statistics*

Out of the 34 banks registered in South Africa, only 12 followed and published the Wolfsberg AML/CFT questionnaire. These included FirstRand Bank, Standard Bank, Mercantile Bank, HSBC and Deutsche Bank. The results indicate that the majority of the banks are foreign controlled and branches of foreign banks. This confirms the notion that foreign controlled banks usually comply with the parent bank's domicile AML/CFT regulations. The Wolfsberg AML/CFT questionnaire, together with the other secondary sources, provided answers to research questions.

The interviews were held with ten experts working within the financial services sector in South Africa. The experts' opinions, therefore, assisted in closing the gaps noted or corroborating findings obtained in the analysis of secondary data.

### *4.2 Main themes*

The main themes generated from the interviews are depicted in Figure 1. These themes, identified through data analysis, serve as the findings of the study.

**Table 2.** Summarised data analysis and approach

| Data | Data sources | Analysis | Research approach |
|---|---|---|---|
| Secondary | Wolfsberg AML/CFT questionnaire, 2021 South Africa Mutual 2021 Evaluation Report, FICA 2001 (Act No. 38 of 2001) as amended, SARB-PA AML/CFT Assessment 2022 Report and SARB-PA Administrative Sanctions Reports | Document analysis | Triangulation |
| Primary | Experts interviews | Thematic | Triangulation |

**Source:** Researchers' own compilation


**Figure 1.**
Main themes of the research study

**Source:** Researchers' own compilation

The main themes generated were third-party vendor, risk-based approach, biometric, Department of Home Affairs (DHA), face-to-face onboarding, PEP and adverse media and transaction monitoring, among others.

*4.3 Research objective 1: to assess the South African banks' individual customer identification and verification practices in the fintech era*

*4.3.1 Secondary data findings.* In terms of identification and verification, the secondary data results show that the banks prohibit the opening of anonymous accounts but verify all the information submitted. Customer details identified and verified for private companies include ownership structure, ultimate beneficiary owners, key controllers and authorised signatories. For individuals, the customer details required and verified are mainly the national identity document. Thus, the banks make every effort to verify the submitted details using third parties. However, with this data collection approach, there is no mention of which third-party sources are used.

*4.3.2 Primary data findings.* The identification and verification of customer details are recognised by Section 21 of the FICA. It was also established that South Africa's financial sector has an integrated system for verification of identity documents with the DHA and Companies and Intellectual Property Commission (CIPC). The DHA and CIPC are the responsible entities in South Africa, with databases for personal identities and company registration details. These two entities are the third-party government sources used by banks to corroborate submitted customer details. This finding concurs with the main theme of using third-party sources.

South African banks have incorporated biometrics during onboarding to include facial recognition and fingerprints. This is supported by various third-party systems to make the onboarding process seamless. The use of biometrics complies with the provisions of FICA and the Protection of Personal Information (POPI) Act. These findings support the main theme of using third-party sources in the verification protocols.

The results suggest that the majority of South African banks still rely on using the traditional ways of onboarding customers, face-to-face or physical. There is a significant shift to digital or remote onboarding, with some banks having both. Remote onboarding was precipitated by the COVID-19 pandemic, prevalent in 2021. In performing the verification of

customer information, client consent must be sought in line with the POPI Act, which requires customer consent when using third-party sources under this protocol.

Primary evidence confirms that South Africa's banks use third-party vendors to assist in corroborating identity and verifying customer details. Technological solutions have been incorporated in performing CDD functions. Thus, the financial services sector has moved its AML/CFT from the rule-based approach to the risk-based approach. This supports the view that in the fintech era, the number of digital transactions and data sets have increased, requiring digital innovation solutions that are currently developed by fintech companies. This assists the banks in AML/CFT regulatory compliance, though care must be taken because fintech companies operate in an unregulated industry and are customer centric.

The primary data findings confirm the third-party sources, which was unanswered during the secondary data analysis. Furthermore, more information was divulged on the legal compliance of the biometric incorporation, integration with the DHA and CIPC databases and customer consent to third-party sources in terms of the FICA and POPI Act. Technological solutions have been incorporated in performing CDD functions, which is now risk-based (enhanced due diligence).

### *4.4 Research objective 2: to determine the South African bank customer's nature and purpose business relationship practices of customer due diligence in the fintech era*

*4.4.1 Secondary data findings.* The results show that on the nature of the business relationship, information is accepted at face value and that the source of wealth is required for PEP clients by most of the banks. Information about sources of income, proof of address, product usage, expected transaction volumes and countries are all incorporated into the risk scoring model that eventually allocates risk class to the customer.

*4.4.2 Primary data findings.* These empirical results confirm that the South African banks are still using third-party vendors in establishing the nature of the business relationship of its customers. These third-party vendor systems act upon the information provided and accepted at face value.

The primary data findings do confirm the secondary data findings on information being accepted at face value. The primary data findings further confirm that third-party vendor systems are used to consolidate the customer information, ultimately giving the risk ratings.

### *4.5 Research objective 3: to examine the South African bank customer's ongoing due diligence measures applied in the fintech era*

*4.5.1 Secondary data findings.* The document analysis verified that all South African banks risk classify their customers, perform transaction screening and monitoring for customers, use automated alerts to screen customers and perform periodic reviews. The results also illustrate that the majority of the banks in South Africa screen customers using both automated and manual systems, with a few either using the manual method or automation only. This shows that financial institutions are in step with the digital era, as manual systems are prone to errors and manipulation.

Banks in South Africa conduct periodic review of customer information based on trigger alerts and know your customer (KYC) renewal timelines. Trigger events include new information about clients such as adverse media, PEP status, volume of transactions and transaction countries. These provide information that can change the risk profile of the customer. It has been noted that banks have in-built risk models that capture all this information.

The document analysis confirmed that financial institutions carry out the process of identifying clients in terms of PEP status. This is done during onboarding and on a

continuous basis. The country has shortcomings on the legal definition of PEP, with the FICA defining a PEP as someone who held a position in the previous 12 months.

*4.5.2 Primary data findings.* The study verified that in South Africa, the PEP identification and adverse media screening process is automated. PEP and adverse media need close monitoring and can bring associated reputational risks to the banks. Thus, risk monitoring and classification of the clients identified as PEP and with adverse media must be enhanced. The study also shows that South African banks have a self-declaration disclosure by customers on the PEP and adverse media status. This contributes to the banks identifying high-risk clients. As per the Mutual Evaluation Report of South Africa, besides the issues on the legal definitions and time limits for PEP, South Africa is not compliant on this aspect. This finding is in agreement with the primary results regarding the issue of time limits.

Transaction monitoring and screening are automated and are used by South African banks in addressing associated AML/CFT risks. The empirical findings show that some use outsourced and others are internally developed. These findings concur with the fintech developments and increase in customer digital transactions that generate massive data sets as reliance is placed on technological solutions reporting systems to detect unusual behaviour.

The primary findings corroborate the legal definitions of the PEP raised in the secondary data analysis. Also, transaction monitoring and screening are pivotal in detecting unusual behaviour. The primary data findings confirm the ongoing monitoring variables as contributing to the customer's risk profile updates.

*5.6 Research objective 4: to evaluate the anti-money laundering/combatting of financing terrorism regulatory enforcement actions effected on South African banks in the fintech era*

*5.6.1 Secondary data findings.* The regulator, SARB:PA conducts risk-based AML/CFT assessments of the 34 banks under its jurisdiction. Accordingly, of the 34 banks in South Africa, 27 are rated medium risk and 7 are rated high risk. Over the period 2012–2019, the regulator conducted on average seven inspections annually. Based on the information, it can be argued that the regulator takes approximately five years to completely inspect all the 34 banks under its regulatory arm. Further information verified that the regulator frequently conducts AML/CFT meetings with the large banks, although the agenda of the meeting and minutes are not made publicly available. Thus, the SARB-PA seems to rely heavily on these meetings rather than conducting onsite inspections.

In 2016, the highest number of AML/CFT regulatory sanctions was received by six banks. These banks include Investec Bank (ZAR 20m for failure to implement a customer screening process) and Standard Bank's Johannesburg branch (ZAR 10m for failure to perform identity and verify customers). During the 2017–2019 period, the number of sanctioned banks dropped, although the average financial penalty per institution varied substantially. The reduced inspections and sanctioned financial institutions from 2017 could be attributed to the legislative amendments to FICA. As of 2022, the highest penalty was imposed on China Construction Bank, amounting to ZAR 75m for failure to identify and verify its clients, among the regulatory deficiencies noted. Of the regulatory penalties instituted, the regulatory deficiencies noted included CDD processes and poor transaction monitoring systems.

*5.6.2 Primary data findings.* The results indicate that regulatory appeal is embedded in the legislation, a clear penalty determination process, a rule-based to a risk-based AML approach and conditional penalties. Thus, after regulatory assessments, an appeal process is set out in FICA and banks can be given conditional penalties. Furthermore, the penalty

determination process is clearly laid out, giving room for both parties to come to an amicable solution. An appeal can arise due to the different legal interpretations of the parties concerned.

Findings from both primary and secondary do concur with risk-based regulatory assessments and the penalties thereof. However, the primary data further revealed that regulatory appeals are usually the result of different legal interpretations among the parties concerned. The analysis of the regulatory deficiencies demonstrated that the trend is increasing in the transaction monitoring systems, with CDD no longer an issue.

## 5. Conclusion

Based on the findings of the study, it is concluded that in South Africa, technological solutions have been incorporated in performing CDD functions, which is now risk-based (enhanced due diligence). Also, legally, South Africa has incorporated biometrics, integration with the DHA and CIPC databases and customer consent to third-party sources in terms of the FICA and POPI Act. There is a shift towards digital banking in South Africa, which will ultimately result in increased data and dynamic risk profiling requiring a risk-based approach to mitigate emerging ML risks. As such, much needs to be done by regulators to foster enhanced due diligence in light of South Africa's recent greylisting by the FATF.

A number of recommendations flow from the study. These are as follows:

### *5.1 Increasing monitoring of customer transactions using technologies*

Compared to traditional banks, digital banks can onboard new clients far more quickly. Customer KYC documents are typically uploaded using smartphones with verification and validation done swiftly. AML/CFT, eKYC and cybersecurity threats are increased due to digital banking necessitating mitigation measures. The financial industry may be able to fight back against this crime if it adopts a multi-layered strategy that includes sophisticated identification verification, intelligent data utilisation and ongoing behavioural monitoring. To monitor consumer activities and swiftly identify possible hazards, digital banks should use Regtech technologies such as artificial intelligence.

### *5.2 Evidence-based Financial Action Task Force recommendations*

It is our considered view that FATF Recommendation 10 needs to be changed to enhanced due diligence, because the CDD provides a static risk-based view and not give an accurate risk exposure assessment given the dynamic risk profiling existing in the era of digital innovations. Thus, the FATF at a global level should revise the FATF guidelines to be informed by research.

### *5.3 Responsive regulations*

AML/CFT regulators need to be pragmatic in responding to the environmentally induced threats posed by digital currencies and digital economies. There is a need to develop adequate and effective regulatory responses to ensure that technological outcomes are met without compromising regulatory objectives. Regulations should not be static but should evolve. The paradigm shift makes regulations, regulatory bodies and financial services effective in meeting their regulatory mandates.

*5.4 Interdisciplinary nature*

Technological innovations have broadened emerging ML risks and risks to the financial system in general. The emerging risks are imminent because of the integrated disciplinary nature in which ML phenomena needs to be addressed. The evolving nature and integration of the disciplines influence how to regulate.

## References

Arasa, R. and Ottichilo, L. (2015), "Determinants of know your customer (KYC) compliance among commercial banks in Kenya", *Journal of Economics and Behavioral Studies*, Vol. 7 No. 2 , pp. 162-175.

Araujo, R. (2009a), "Are labour contracts efficient to combat crime?", *Journal of Financial Crime*, Vol. 16 No. 3, pp. 255-261.

Araujo, R. (2009b), "Assessing the efficiency of the Brazilian anti-money laundering regulation: a game theoretic approach", *Revista de Economia Do Mackenzie*, Vol. 7 No. 1, pp. 30-42.

Araujo, R.A. (2010), "An evolutionary game theory approach to combat money laundering", *Journal of Money Laundering Control*, Vol. 13 No. 1, pp. 70-78.

Bamberger, K.A. (2016), "Foreword: technology's transformation of the regulatory endeavor", *Berkeley Technology Law Journal*, Vol. 26 No. 3, pp. 1315-1320.

Beebeejaun, A. and Lubnaa, D. (2022), "A critical analysis of the anti-money laundering legal and regulatory framework of Mauritius: a comparative study with South Africa", *Journal of Money Laundering Control, (Forthcoming)*, Vol. 26 No. 2.

Bethelihem, A. (2019), *Challenges and Practices of AML/CFT: The Case of Ethiopian Commercial Banks*, St Mary's University, Addis Ababa.

Betts-LaCroix (2010), "Hype chasm", available at: http://blog.evocator.org/2010/04/hype-chasm.html (accessed 16 August 2021).

Bouvatier, V. (2014), "Heterogeneous bank regulatory standards and cross-border supply of financial services", *Economic Modelling*, Vol. 40, pp. 342-354.

Bushman, R.M. (2016), "Transparency, accounting discretion, and bank stability", *Economic Policy Review*, Vol. 2016, pp. 129-149.

Butler, T. and Brooks, R. (2018), "On the role of ontology based regtech for managing risk and compliance reporting in the age of regulation", *Journal of Risk Management in Financial Institutions*, Vol. 11 No. 1, pp. 19-33.

Cash, D. (2020), "Sigma ratings: adapting the credit rating agency model for the anti-money laundering world", *Journal of Money Laundering Control*, Vol. 23 No. 1, pp. 1-10.

Chitimira, H. and Munedzi, S. (2021), "Selected challenges associated with the reliance on customer due diligence measures to curb money laundering in South African banks and related financial institutions", *Journal of Comparative Law in Africa*, Vol. 8 No. 1, pp. 42-66.

Chitimira, H. and Munedzi, S. (2022), "Overview international best practices on customer due diligence and related anti-money laundering measures", *Journal of Money Laundering Control, (Forthcoming)*, Vol. 26 No. 7.

Christie, R. (2018), "Setting a standard path forward for KYC", *The Capco Institute Journal of Financial Transformation*, Vol. 47 No. 4, pp. 155-164.

Cindori, S. and Petrovic, T. (2018), "The significance of assessing money laundering risk as a part of auditing operations", *Athens Journal of Business & Economics*, Vol. 4 No. 1, pp. 79-91.

Clarke, A.E. (2021), "Is there a commendable regime for combatting money laundering in international business transactions? ", *Journal of Money Laundering Control*, Vol. 24 No. 1, pp. 163-176.

Cutter, H. (2018), "DoJ targets duplicate penalties through increased coordination", *The Wall Street Journal*, available at: www.wsj.com/articles/doj-targets-duplicative-penalties-through-increased-coordination-1525880371 (accessed 10 August 2022).

Demetis, D.S. (2010), *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach*, Edward Elgar, Cheltenham.

Demetriades, P.O. and Rousseau, P.L. (2016), "The changing face of financial development", *Economics Letters*, Vol. 141, pp. 87-90.

ElYacoubi, D. (2020), "Challenges in customer due diligence for banks in the UAE", *Journal of Money Laundering Control*, Vol. 23 No. 2, pp. 527-539.

Esoimeme, E.E. (2015), *The Risk Based Approach to Combating Money Laundering and Terrorist Financing*, Eric Press, New York, NY.

Eusepi, S. (2004), "Does Central bank transparency matter for economic stability?", Paper No. 173, Computing in Economics and Finance 2004, Society for Computational Economics.

FATF (2012), High-level synopsis of the stocktake of the unintended consequences of the FATF standards, Paris, available at: www.fatf-gafi.org/media/fatf/documents/Unintended-Consequences.pdf (accessed 26 December 2022).

FATF (2014), Virtual Currencies. Key Definitions and Potential AML/CFT Risks: FATF, Paris, available at: www.fatf-gafi.org/en/publications/Methodsandtrends/Virtual-currency-definitions-aml-cft-risk.html (accessed 19 May 2022).

FATF (2018), *International Standards on Combatting Money Laundering and the Financing of Terrorism & Proliferation*, FATF, Paris, France.

Fennie, J. (2010), "Understanding Gartner's hype cycles, 2010, s.l.: Gartner research report FIC", *Guidance Note 7 on the Implementation of Various Aspects of the Financial Intelligence Centre Act, 2001 (Act 38 of 2001)*, Financial Intelligence Centre South Africa, Pretoria, p. 2017.

Ferwerda, J. (2009), "The economics of crime and money laundering: does anti-money laundering policy reduce crime?", *Review of Law & Economics*, Vol. 5 No. 2, pp. 903-929.

Fulop, M.T., Dan, I.T., Constatin, A.I., Sorinel, C., Teodera, O.B. and Stanescu, S. (2022), "FinTech accounting and industry 4.0: future proofing or threats to the accounting profession", *Journal of Business Economics and Management*, Vol. 23 No. 5, pp. 997-1015.

Gara, M. and Pauselli, P. (2020), "Looking at 'crying wolf' from a different perspective: an attempt at detecting banks under- and over-reporting of suspicious transactions", *Italian Economic Journal*, Vol. 6 No. 2, pp. 299-324.

Gaviyau, W. and Sibindi, A.B. (2023), "Customer due diligence in the fintech era: a bibliometric analysis", *Risks*, Vol. 11 No. 1, pp. 11-28.

Gleb, A. (2016), "Balancing financial integrity with financial inclusion: the risk-based approach to 'know your customer'", *CDG Policy Paper 74*, Centre for Global Development, Washington, DC.

Gomber, P., Koch, J.A. and Siering, M. (2017), "Digital finance and fintech: current research and future research directions", *Journal of Business Economics*, Vol. 87 No. 5, pp. 537-580.

Harry, J. and Suntura, C. (2020), "Customer identification in currency exchange companies as per FATF recommendations", *Journal of Money Laundering Control*, Vol. 23 No. 1, pp. 96-102.

Healy, P. and Palepu, K. (2001), "Information asymmetry, corporate disclosure and the capital markets: a review of the empirical disclosure literature", *Journal of Accounting and Economics*, Vol. 31 Nos 1/3, pp. 405-440.

IMF (2015), *The IMF and Fight Against Money Laundering and Financing of Terrorism*, IMF, Washington, DC.

Isolauri, E.A. and Ameer, I. (2022), "Money laundering as a transnational business phenomenon: a systematic review and future agenda", *Critical Perspectives on International Business (Forthcoming)*, Vol. 19 No. 3.

Jayasekara, S.S.D. (2021), "Risk-based AML/CFT regulations for effective supervision", *In Money Laundering and Terrorism Financing in Global Financial Systems*, IGI Global, Pennsylvania, USA, pp. 207-237.

Johari, R.J., Zul, N.B., Talib, N. and Hussin, S.A.H.S. (2020), "Money laundering: customer due diligence in the era of cryptocurrencies", *1st International Conference on Accounting, Management and Entrepreneurship (ICAMER 2019)*, *Atlantis Press*, pp. 130-135.

Juntunen, J. and Teittinen, H. (2022), "Accountability in anti-money laundering – findings from the banking sector in Finland", *Journal of Money Laundering Control, (Forthcoming)*, Vol. 26 No. 2.

Kavuni, S.A. and Milne, A. (2019), "Fintech and the future of financial services: what are the research gaps?", CAMA Working Paper 18/2019, Australia National University, Canberra.

Kundid, A. and Rogosic, A. (2012), "E-transparency of Croatian banks: determinants and disclosure contents", *Economic Research-Ekonomska Istraživanja*, Vol. 25 No. sup1, pp. 86-116.

Lai, P.C. (2017), "The literature review of technology adoption models and theories for the novelty technology", *Journal of Information Systems and Technology Management*, Vol. 14 No. 1, pp. 21-38.

Maguchu, P. (2018), "Revisiting money-laundering legislation in Zimbabwe and the role of international organisations", *African Security Review*, Vol. 27 Nos 3/4, pp. 278-290.

Martínez-Sánchez, J.F., Venegas-Martínez, F. and Pérez-Lechuga, G. (2022), "Money laundering risk management in multiple-purpose financial institutions in Mexico: a Bayesian network approach", *Journal of Money Laundering Control (Forthcoming)*, Vol. 26 No. 4.

Masciandaro, D. (1999), "Money laundering: the economics of regulation", *European Journal of Law and Economics*, Vol. 7 No. 3, pp. 225-240.

Matsuo, A. and Staines, K. (2020), "Ten key regulatory challenges for 2020", available at: https://advisory.kpmg.us/articles/2019/ten-key-challenges-2020.html (accessed 14 August 2023).

Mniwasa, E. (2019), "Money laundering control in Tanzania: did the bank gatekeepers fail to discharge their obligations? ", *Journal of Money Laundering Control*, Vol. 22 No. 4, pp. 796-835.

Neuman, M. (2005), "The compact city fallacy", *Journal of Planning Education and Research*, Vol. 25 No. 1, pp. 11-26.

Osifo, S.J. (2020), "Customer relationship management as a tool for improving bank performance and nation building", *The Academy of Management Journal*, Vol. 15, pp. 10-24.

Oztas, B., Deniz, C., Festus, A. and Marcin, B. (2022), "Enhancing transaction monitoring controls to detect money laundering using machine learning", available at: http://eprints.bournemouth.ac.uk/37921/1/Oztas_et_al_ExtendedAbstract_ICEBE22.pdf (accessed 30 December 2022).

Phanwichit, S. (2018), "Fintech and causing customers to comply with anti-money laundering law", *PSAKU International Journal of Interdisciplinary Research*, Vol. 7 No. 2, pp. 1-8.

Raweh, B.A., Erbao, C. and Shihadeh, F. (2017), "Review the literature and theories on antimoney laundering", *Asian Development Policy Review*, Vol. 5 No. 3, pp. 140-147.

Rogers, E.M. (1962), *Diffusion of Innovations*, Free Press, New York, NY.

SARB (2022), "South Africa Reserve Bank Prudential Authority AML/CFT Banking Sector Assessment Report: South Africa Reserve Bank".

Schoonenboom, J. and Johnson, R.B. (2017), "How to construct a mixed methods research design", *KZfSS Kölner Zeitschrift Für Soziologie Und Sozialpsychologie*, Vol. 69 No. S2, p. 107.

Sharif, A., Ranzi, M., Carbone, R., Sciaretta, G., Marino, F.A. and Ranise, S. (2022), "The eIDAS regulation: a survey of technological trends for European electronic identity schemes", *Applied Sciences*, Vol. 12 No. 24, p. 12679.

Shuler, K. (2012), "The Gartner hype cycle & technology adoption lifecycle explained (using NoC technology)", available at: https://www.arteris.com/blog/bid/89308/the-gartner-hype-cycle-technology-adoption-lifecycle-explain (accessed 14 August 2023).

Sujee, Z.J. (2016), "A study of the anti-money laundering framework in South Africa and the United Kingdom", PhD Thesis, University of Pretoria, Pretoria.

Sultan, N. and Mohameed, N. (2022), "Challenges for financial institutes in implementing robust customer due diligence in Pakistan", *Journal of Money Laundering Control (Forthcoming)*.

Sunarmi, S., Sukarja, D. and Lubis, T.M. (2022), "Implementation of customer due diligence principles on financial service companies in preventing and eradicating criminal action of money laundering in medan", *Jurnal Mercatoria*, Vol. 15 No. 2, pp. 104-117.

Tadesse, S. (2006), "The economic value of regulated disclosure: evidence from the banking sector", *Journal of Accounting and Public Policy*, Vol. 25 No. 1, pp. 32-70.

Takats, E. (2007), "A theory of 'crying wolf': the economics of money laundering enforcement", International Monetary Fund Working Paper WP07(81), IMF, Washington, DC.

Teddlie, C. and Tashakkori, A. (2010), "Overview of contemporary issues in mixed methods research", *Sage Handbook of Mixed Methods in Social and Behavioral Research*, Vol. 2, pp. 1-44.

Teichmann, F.M.J. and Wittmann, C. (2022), "Money laundering in the United Arab Emirates: the risks and the reality", *Journal of Money Laundering Control (Forthcoming)*, Vol. 26 No. 4.

Trajkovski, G. and Nanevski, B. (2019), "Customer due diligence – focal point of anti-money laundering process", *Journal of Sustainable Development*, Vol. 5 No. 12, pp. 39-50.

Viritha, B. and Mariappan, V. (2013), "Compliance with AML & CFT guidelines: a review of implementation in banks", *Pacific Business Review International*, Vol. 5 No. 10, pp. 1-10.

Viritha, B., Mariappan, V. and Haq, I.U. (2015), "Suspicious transaction reporting: an Indian experience", *Journal of Money Laundering Control*, Vol. 18 No. 1, pp. 2-16.

Watts, R.L. and Zimmerman, J.L. (1986), "Positive accounting theory", *The Accounting Review*, Vol. 65 No. 1, pp. 131-156.

Yim, H.C. and Lee, P.I. (2018), "Updates on Hong Kong's anti-money laundering laws", *Journal of Money Laundering Control*, Vol. 21 No. 3, pp. 98-110.

Zetzsche, D.A., Warner, D., Buckley, R. and Weber, R. (2019), "The future of data-driven finance and RegTech: lessons from EU big bang II", European Banking Institute Working Paper Series 2019/35, UNSW Law Research Paper No. 19-22, University of Luxembourg Law Working Paper No. 005-2019, University of Hong Kong Faculty of Law Research Paper No. 2019/004.

**Corresponding author**
Athenia Bongani Sibindi can be contacted at: sibinab@unisa.ac.za