

Article

Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique

William Gaviyau  and Athenia Bongani Sibindi * 

Department of Finance Risk Management and Banking, University of South Africa (UNISA), P.O. Box 392, Pretoria 0003, South Africa; wgaviyau1@gmail.com

* Correspondence: sibinab@unisa.ac.za; Tel.: +27-(0)-12-429-3757; Fax: +27-(0)-86-569-8848

Abstract: Money launderers prefer to use financial services as the ideal medium for laundering. This study aimed to provide an overview of the global AML/CFT regulations, application and how they should evolve in this dynamic environment. To gather more insight, a qualitative study was undertaken with relevant documents analysed. The main finding was that country implementation of the global AML/CFT regulations differed due to political and economic factors, amongst others. While the various AML/CFT enforcements done by sampled countries were mainly cease and desist orders and monetary penalties that were publicised, the drawbacks of global AML/CFT regulations centred on the application of these regulations and emerging trends. These include, among other definitions of money laundering, reference to the three stages of money laundering, the link between penalty and violations, technological innovations and regulation paradigm shift, cyber-attacks, and data privacy. This study contributes to the application and growing body of knowledge in that the advent of technology has resulted in better consumer experiences, new payment platforms, products and services. However, these innovations have broadened emerging money laundering risks and risks to the financial system in general. Hence, there is a need to conduct research-based FATF recommendations, as risk is dynamic and not static.

Keywords: FATF; AML/CFT; money laundering; risk; FinTech; RegTech; banking regulations



Citation: Gaviyau, William, and Athenia Bongani Sibindi. 2023. Global Anti-Money Laundering and Combating Terrorism Financing Regulatory Framework: A Critique. *Journal of Risk and Financial Management* 16: 313. <https://doi.org/10.3390/jrfm16070313>

Academic Editor: Badar Nadeem Ashraf

Received: 18 May 2023
Revised: 17 June 2023
Accepted: 26 June 2023
Published: 28 June 2023



Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Technology poses a significant threat to banking and regulatory systems (Clarke 2021; Anagnostopoulos 2018). The rapid pace of technology changes has left regulators with the huge task of developing adequate regulatory responses, even though they may not understand them (Ofoeda 2022; Groepe 2017). Most of the current banking regulations apply to the traditional banking model. However, in the digital innovation era, regulators still require banks to apply the same risk management practices to the current digital banking practices. Failure to apply culminates in non-compliance. Fintech is still emerging, evolving and disrupting the financial services industry (Nejad 2022; Anagnostopoulos 2018; Dong 2017; Brummer 2015). Based on the old regulations, banks are still expected to have sound AML practices. This is detrimental. The global AML/CFT regulatory framework is anchored on the FATF's 40 recommendations. The FATF collaborates with other international organisations in the sharing and dissemination of AML/CFT associated information.

Money launderers prefer to use financial services as the ideal medium for laundering. Accordingly, FATF designed recommendations 1 to 40 on which country AML/CFT regulations are based and benchmarked. FATF recommendations are universally acceptable guiding standards in the regulatory design to counter money laundering and the risks of financing terrorism. The implementation is country dependent, though drawing from the FATF recommendations. Accordingly, each country is supposed to come up with customised legislation and implementation thereof. Failure to implement results in the country being used as a conduit for money laundering and terrorism funding, which goes

against the global shared objective. AML/CFT weaknesses affect the financial system’s integrity and national security (Teichmann and Wittmann 2022; Cutter 2017).

After the global financial crisis, financial regulations continue to be modified and reviewed with the aim of combatting money laundering, protecting consumers and ensuring integrity in the financial system. As such, this paper sought to detail the global AML/CFT regulations, application and how they should evolve in this dynamic environment.

This paper has 8 sections. Section 1 is the introduction, with Section 2 providing an overview of money laundering. Section 3 provides the theoretical and empirical literature, and Section 4 discusses the research approach adopted. Section 5 outlines FATF recommendations, country implementation and regulatory enforcements. Section 6 outlines the critique concerning the current AML/CFT regulatory framework, Section 7 is the conclusion, and lastly, Section 8 discusses the limitations and areas of future research.

2. Overview of Money Laundering

Economic players are rewarded for using factors of production (Littrell 2022; Mohr and Lewis 2008; Masciandaro 1999). Rewards can be earned legally or illegally but still need to be accounted for under the economic performance statistics. However, illegally earned funds remain difficult to account for due to the falsification of income sources (Clarke 2021; Sotande 2018; Arnone and Borlini 2010). The sources of dirty money include (among others) corruption, fraud, tax evasion, theft and bribery. Historically, money laundering has gone through three stages. These are placement, layering and integration. However, with digital innovations, money laundering can occur at any of these three stages. Each stage has associated activities, which are shown in Figure 1. Typical money laundering activities at each stage are illustrated in the schematic map below.

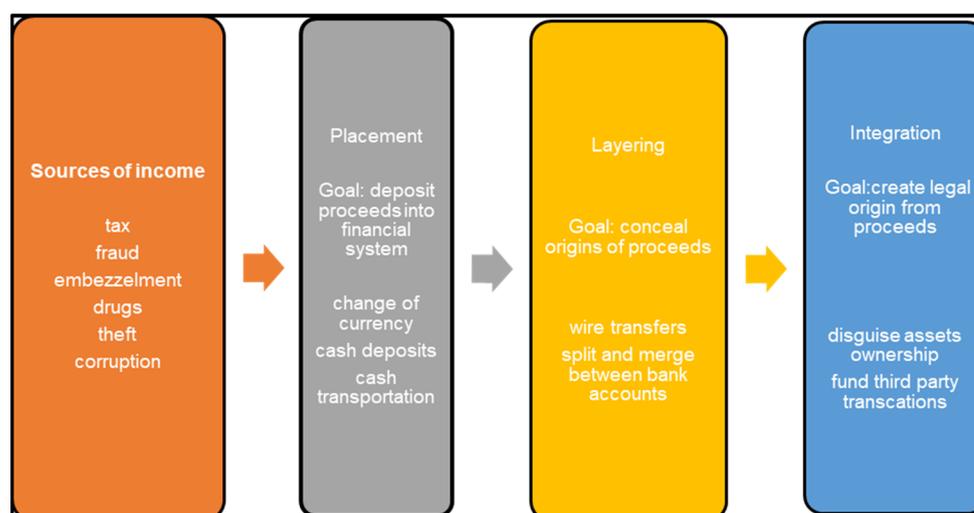


Figure 1. Activities under the money laundering process. Source: Researcher’s own conceptualisation.

2.1. Placement Stage

This is the first stage through which dirty money is infused into formal banking channels in various forms (Clarke 2021; Whisker and Lokanan 2019; Papanicolaou 2015). The aim at this phase is to place illicit money into the legitimate banking system and relieve the launderer of holding large amounts of money. Methods used at the placement stage include smurfing; deposits using fake identity documents; refining; cash transportation, and cash rich business (Papanicolaou 2015). These methods are discussed below.

2.1.1. Physical Cash Deposit and Smurfing

Dumitrache and Modiga (2011) postulate that physical cash deposits and/or smurfing are usually utilised by money launderers. To circumvent meeting AML/CFT cash or suspicious reporting obligations, money launderers opt for smurfing (Choo et al. 2014). The

breaking down of illegally earned funds into smaller deposits that are below cash reporting thresholds is known as smurfing. Similarly, with current electronic forms of money substituting for cash deposits, this stage can become so obvious to overlook within the monitoring system (Whisker and Lokanan 2019; Dumitrache and Modiga 2011; Filipkowski 2008). Mynhardt and Johan (2013) observed that huge cash deposits have been associated with cash-based economies compared to digital-based economies.

At the placement stage with poor AML/CFT regulatory oversight, incorrectly captured customer details create money laundering risks (Collin 2020; Whisker and Lokanan 2019). These include failure to risk profile customers, resulting in financial institutions failing to place appropriate mitigatory measures and being complicit in money laundering.

2.1.2. Fake Identity Documents and Refining

Another form commonplace in money laundering is when deposits are made using fake identity documents and names (Arnone and Borlini 2010). This, however, exerts pressure on financial institutions and KYC principles. As part of the CDD measures, banks need to verify and authenticate submitted customers' national identity documents (Sultan and Mohamed 2022; Arasa and Ottichilo 2015). Verification and authentication minimise the risk of wrongly profiling the customers. Launderers can also opt for refining, which entails using high denominated values of currency for smuggling purposes (Trajkovski and Nanevski 2019; Hopton 2009). In the fight against higher denominations being used for money laundering purposes and cash smuggling, the European Central Bank phased out the issuance of Euro 500 denominations in 2018 and replaced them with 200 and 100 denominations (European Commission 2016). Financial institutions need to perform strict CDD procedures during onboarding and throughout the course of the financial relationship.

2.2. Layering

In this second stage of money laundering, the money launderers disguise original sources of illegal funds by moving funds from one location to another (Moiseienko 2022; Whisker and Lokanan 2019; Papanicolaou 2015). Ryder (2012) posits that layering involves avoiding an audit trail by making payments or purchasing immovable property through electronic transfers to another bank, either locally or internationally. At this stage, the aim is to create less traceability suspicion to the original, much as possible.

Money launderers can structure financial transactions to conceal audit trails by breaking down the original amount into smaller transactions to deceive possible investigators (Whisker and Lokanan 2019). Stessens (2000) posits that for the transaction to be successful at the layering stage, the money launderers need to do as many electronic banking transactions as possible. Due to technological innovations that enable instant international and local bank transfers, at this stage regulators can fail to detect and or investigate possible money laundering issues (Whisker and Lokanan 2019; Dumitrache and Modiga 2011). Launderers can opt to use parallel banking systems, such as Hawala/Hundi and illegal international money transfers (Mniwasa 2019; Papanicolaou 2015) if they are determined to cover their trails.

Characteristically, money launderers at the layering stage are not concerned with brokerage or transfer fees and investment losses (Anagnostopoulos 2018). This shows that the only motive of money launderers at this stage is that the original source of funds is concealed. Another characteristic is the increased frequency of cross-border transactions in the form of investments or remittances, which could be an indicator of money laundering at the layering stage (Sileshi 2022). Thus, proper CDD measures need to be exercised on customers during onboarding and thereafter.

2.3. Integration

According to the three-stage process, this is the final stage in which money reappears into the economy through investment (Kaur and Sandhu 2022; Papanicolaou 2015). The money is returned to criminals through several methods and is used for other purposes.

The aim is to reunite in a way that does not draw attention and appears as if the source of funds is legitimate (Whisker and Lokanan 2019). Launderers can use complex methods to avoid suspicions, such as international funds transfer and direct or offshore investments (Suntura Clavijo 2020; Al-Nuemat 2014). At this stage, launderers constantly move funds to elude detection and exploit legal loopholes in the country's AML/CFT legislation.

Most money launderers have offshore accounts and make transnational investments to disguise sources of funds (Sultan and Mohamed 2022; Bofondi and Gobbi 2017; Papanicolaou 2015). Indeed, cross-border investments need to be scrutinised. However, the challenge lies in non-cooperation or cooperation among nations (Mathuva et al. 2020; Naheem 2018; Araujo 2010; Masciandaro 1999). Cross-border payments and investments pose a considerable challenge to financial institutions and anti-money laundering efforts (Sultan and Mohamed 2022; Basel Committee on Bank Supervision 2018). Furthermore, increased cross-border investments and international funds transfer combined with poorly performed CDD procedures and anonymity at the placement stage all pose significant threats to the financial sector and ultimately financial integrity (Whisker and Lokanan 2019; Solin and Zerzan 2010).

3. Theoretical and Empirical Literature

This study is anchored on the three theories, namely transparency stability, systems theory and systems theory. Empirical evidence was obtained from developed and developing countries.

3.1. Theories

First, transparency stability theory argues that information asymmetries do exist in the financial sector (Tadesse 2006). Thus, it places emphasis on the regulatory disclosures about AML/CFT regulatory penalties enforced in the banking sector. Second, systems theory, as advanced by Demetis (2010), posits that the money laundering domain consists of systems and subsystems. Systems consist of a regulatory framework—transnational, national and local. The subsystem has political, legal and economic factors. The domain assists in identifying the recommendations underpinning the study from the FATF 40 recommendations and associated AML/CFT regulatory compliance. Finally, model of IT implementation process by Cooper and Robert (1990), which is based on innovation, technological diffusion and organisational change. The theory was designed and developed when the banking systems technologies were not integrated, while the current and future banking systems have integrated systems. Thus, when integrated, it can explain the behaviour of financial sector players in responding to the Fintech developments of mitigating emerging money laundering risks.

3.2. Empirical

An empirical review of studies emanating from developed countries illustrated that regulatory developments have been initiated and are at various stages of being utilised or tested. Anichebe (2020) and Yuen (2018) concur on the use and development of these regulatory technologies for compliance to the AML/CFT regulations. Meiryani et al. (2022) argued that regulatory technology (RegTech) remains an essential component in effectively curbing money laundering. Progressively, in line with recommendation 15, a regulatory framework that takes into consideration crypto assets has been formulated and is currently used in Malta (Buttigieg et al. 2019). However, some developing countries still lag behind and acknowledge the existence of regulatory arbitrages and emergent risks (Anichebe 2020; Magarura 2013).

In developing countries, the empirical literature established that countries are being forced to respond to technological innovations. From the evidence, knowledge gaps exist in the domestication of AML/CFT regulations and the incorporation of technology innovations into the banking sector. Another is the adoption of risk-based approaches to AML/CFT. Studies in developing countries are still scant, suggesting some need for more

collaborations. [Gaviyau and Sibindi \(2023\)](#) documented that the AML/CFT subject has few collaborations due to the technical nature of the subject. Thus, few collaborations indicate more scope for researchers, while the technological lags suggest that money launderers have an opportunity to defraud customers and banking institutions alike.

4. Research Approach

To gather more insights into the global AML/CFT regulations and applications, a qualitative approach was adopted. This involved undertaking a structured literature review as well as document analysis through applicable legislation, publicised AML/CFT regulatory enforcements, and related developments. Firstly, information was obtained from the selected country's AML/CFT regulator and associated websites. To achieve a balanced approach, the selected countries were from both developed and developing countries. This enabled the identification of legislative gaps between the two categories of countries. This was followed by an analysis of the published regulatory enforcements as specified in the AML/CFT regulations. In line with the transparency stability theory, regulators have a mandate to publicly disclose issues under their regulatory space, in this case AML/CFT issues ([Kirakul et al. 2021](#); [Tadesse 2006](#)). Regulatory disclosures support regulatory mandates, such as consumer protection and financial stability. [Armitage and Keeble-Allen \(2008\)](#) posit that a structured literature review summarises the impactful, innovative and latest developments on the subject under study.

5. FATF Recommendations, Country Implementation and Regulatory Enforcement

The section discusses FATF-associated issues related to the organisation structure, recommendations and implementations. The AML/CFT regulatory enforcements is also to be discussed.

5.1. Financial Action Task Force (FATF) Organisation Structure

The Financial Action Task Force (FATF) is an organisation under the auspices of the Organisation for Economic Co-operation and Development (OECD) that specialises in offering measures to combat money laundering ([De Koker 2022](#); [FATF 2012](#)). FATF was established in 1989 as an intergovernmental body involving over 180 countries. Its mandate is designed to establish benchmarks that encourage the effective implementation of regulatory, operational and legal measures to combat risks associated with money laundering in the international financial system ([FATF 2021](#); [FATF 2012–2019](#)).

Precipitating factors gave way to the establishment of FATF. Some of these factors included failure of domestic regulations to deal with challenges of increased cross-border transactions, globalisation and diaspora remittances, amongst others ([Sujee 2016](#)). Associated money laundering approaches adopted at the national or community levels without regional and international support have limited influence ([Mniwasa 2019](#); [Sujee 2016](#)). The coordinated approach envisaged in the international bodies helps in addressing the challenges at the global level.

The coordination of FATF's international activities is done through regional and international bodies ([Jones and Knaack 2019](#); [Ryder 2012](#); [FATF 2012](#)). The regional bodies include the Eastern and Southern African Anti-Money Laundering Group (ESAAMLG); Asia Pacific Group (APG); CFATF for Caribbean countries; GABAC for the Economic and Monetary Community of Central Africa; and GIABA for countries in Western Africa. International private sector bodies have supported and recommended the adoption of the FATF 40 recommendations to curb the risks associated with money laundering ([Arnone and Borlini 2010](#)). Among others international bodies include the Basel Committee on Banking Supervision, International Monetary Fund (IMF), United Nations (UN), World Bank Wolfsburg Group, Offshore Group of Banking Supervisors, Financial Stability Forum of Offshore Financial Centres, International Organisation of Securities Commission and Egmont Group of Financial Intelligence Units.

FATF was mandated to develop an assessment framework for the member countries’ level of compliance and implementation regarding the AML/CFT regulatory framework (GIABA 2015; FATF 2012). Assessments are carried out by the regional bodies of the FATF and shared with the countries. Effective cooperation is the panacea to resolving the AML problem. Sherman (1993) argues that “the fight against money laundering cannot be the sole responsibility of government and law enforcement agencies. If these activities are to be suppressed and hopefully in the long term substantially eliminated, it will require the collective will and commitment of the public and private sector working together.” Progressively, the views of Sherman (1993) have been supported by Dobrowolski and Sułkowski (2020). Thus, worldwide AML/CFT efforts through the FATF and international partners are aimed at enhancing the resilience of financial institutions in curbing money laundering and related crimes.

5.2. FATF Recommendations

FATF, as part of its mandate, established a minimum regulatory criterion known as the forty (40) recommendations in combating money laundering and terrorist financing (De Koker 2022; Sujee 2016). These recommendations provide regulatory floors, not ceilings, to be met in order to be compliant (Held 2019). However, depending on the country’s risk appetite, they can enhance or use the 40 recommendations as the basis for the country’s AML regulations. These recommendations are not internationally binding, even though most countries have made a political commitment to abide by the recommendations (Sujee 2016; FATF 2012). Johansson et al. (2019) recommend that institutions operating in uncertain environments are largely dependent on the political economy. In the long run, this uncertainty creates problems for financial institutions (Hill 2018).

As shown in Table 1, the 2012 recommendations cover legal systems, measures taken to prevent ML/TF, and international cooperation. FATF recommendations have been progressively revised from the 1990 initial recommendations to the 2012 and these still have been amended in 2020 (Dobrowolski and Sułkowski 2020; FATF 2012–2019). De Koker (2022) concurs with De Koker and Turkington (2016) that the initial FATF recommendations were not informed by research but were based on the small group of people’s expertise and their subjective perceptions. Admittedly, these recommendations are continually revised to reflect the ever-changing environment and anticipated future threats posed by money launderers.

Table 1. Summarised 2012 FATF Recommendations.

Recommendation	Theme Area Covered
1–3	Legal Systems
4–25	Approaches by the Financial Institutions and Non-Financial Institutions to prevent Money Laundering and Terrorist Financing
26–34	Institutional and other controls in ML/TF defense
35–40	International Cooperation

Source: Researchers summary.

As shown in Table 2, the revised forty recommendations include: risk identification; AML policy and domestic coordination; preventative measures for designated institutions; establishing the powers and responsibility for competent authorities and facilitation of international cooperation. Despite the comparative differences between the initial and revised recommendations, Mathuva et al. (2020) and Maguchu (2018) recognise that the revised recommendations address emerging threats and strengthen existing obligations. De Koker (2022) argues that FATF should conduct evidence-based standard setting and not rely solely on the expertise of FATF members. As part of regulatory impact assessment, this contributes to policymaking (OECD 2022). The next section discusses the countries’ FATF 40 implementations.

Table 2. Summarised Revised 2022 FATF Recommendations.

Recommendation	Theme Area Covered
1–2	Policies and Coordination for AML/CFT
3–4	Confiscation and Money Laundering
5–8	Terrorist Financing and Financing of Proliferation Financing proliferation of terrorism
9–23	Preventive Approaches
24–25	Beneficial Ownership and Transparency of Legal Entities and Arrangements
26–35	Competent Authorities Powers and Responsibilities
36–40	International Cooperation

Source: Researcher’s summary of developments.

5.3. Selected Countries’ Implementation of FATF 40 Recommendations

FATF recommendations are universally acceptable guiding standards in the regulatory design to counter money laundering risks (FATF 2021; Jones and Knaack 2019; Afande and Maina 2015; Arnone and Borlini 2010). Furthermore, FATF conducts periodic inspections of member countries and evaluates the progress thereof (Littrell 2022; GIABA 2015; Ryder 2012; FATF 2012). However, due to country environment factor differentials, the FATF recommendations are perceived as internationally acceptable and the basis on which countries can customise accordingly.

Afande and Maina (2015) and Maguchu (2018) affirm that countries need to implement the FATF recommendations in line with the country’s environment. The implementation of the FATF recommendations has resulted in AML/CFT legislation. However, the level of implementation differs from country or region. Below are some of the implementations to date by Botswana, Namibia, South Africa, Zambia, Zimbabwe and the United Kingdom.

5.3.1. Botswana

Legislative instruments dealing with ML/TF in Botswana are shown in Table 3. The money laundering activities are coordinated and planned by the Financial Intelligence Agency of Botswana (FIAB). FIAB activities include policy formulation, regulation, supervision, research, informing and educating the public about money laundering conduits and possibilities in Botswana as a country (Government of Botswana 2018). The FIAB derives its powers from the country’s Financial Intelligence Act of 2009.

Table 3. Botswana legislation dealing with Anti-Money Laundering.

Country	Legislation Dealing with AML/CFT
Botswana	The Financial Intelligence (Amendment) Act 2018, the Financial Intelligence (Amendment) Regulations 2018, and the Financial Intelligence Act 2009; Regulations for Combating Terrorism (Implementing UN Security Council Resolutions), 2020; The Proceeds of Crime Act, the Counter Terrorism Act, and other laws

Source: Researcher’s Own Construction.

5.3.2. Namibia

Namibia has three pieces of legislation dealing with ML/FT (Namibia Financial Intelligence Centre 2017). These legislative instruments are shown in Table 4. Namibia’s FIA is legally mandated to oversee the fighting of money laundering and terrorism financing in the country, which promotes the integrity and stability of the financial system.

Table 4. Namibia’s legislation dealing with Anti-Money Laundering.

Country	Legislation Dealing with AML/CFT
Namibia	The Prevention of Organized Crime Amendment Act, 2008 as modified; the Financial Intelligence Act of 2012 (Act No. 13 of 2012); and the Prevention and Combating of Terrorist and Proliferation Activities Act of 2014.

Source: Researchers’ Own Construction.

5.3.3. South Africa

In line with the FATF recommendations, South Africa passed several legislations to deal with ML/FT as shown in Table 5. All of these legislations are interlinked to ensure that no legal loopholes exist (Sujee 2016). FICA and POCA are closely interlinked.

Table 5. South Africa’s legislation dealing with Anti-Money Laundering.

Country	Legislation Dealing with AML/CFT
South Africa	The South African Police Service Act (SAPS) 68 of 1995, the Financial Intelligence Centre Act (FICA), the Protection of Constitutional Democracy against Terrorist and Related Activities Act (POCDATARA), and the National Strategic Intelligence Act (NIA) 39 of 1994, Preventing Organized Crime Act (POCA).

Source: Researchers’ Own Construction.

FATF and ESAAMLG jointly evaluated South Africa in 2009. The report concluded in terms of the FATF recommendations, South Africa was compliant with nine, largely compliant with thirteen, partially compliant with nineteen, and non-compliant with seven. South Africa was further placed under the regular follow-up process. The 2021 Mutual Evaluation report concluded that South Africa was largely compliant with seventeen recommendations, partially compliant with fifteen recommendations, compliant with three recommendations and not compliant with five recommendations. Comparing the 2009 and 2021 mutual evaluation reports, South Africa progressively made concerted efforts to ensure compliance with the forty FATF recommendations. Even though significant progress has been made in addressing money laundering threats, a lot of time and resources are needed (Sujee 2016). Clearly, the existence of legal framework does not guarantee its effectiveness or adequacy (Mniwasa 2019; Maguchu 2018; Sujee 2016).

5.3.4. Zambia

As shown in Table 6, Zambia has various pieces of legislation dealing with financial crimes. These include the establishment of the Financial Intelligence Agency and measures addressing money-laundering and terrorism financing threats. AML legislation is enforced by Zambia’s Financial Intelligence Agency (ZFIA) in liaison with other regulatory bodies (Simwayi and Haseed 2011). ZFIA derives supervisory oversight from the Financial Intelligence Centre Act 46 of 2010, while money laundering is defined and criminalised in the Prohibition and Prevention of Money Laundering Act 44 of 2010 as amended.

Table 6. Zambia’s legislation dealing with Anti-Money Laundering.

Country	Legislation Dealing with AML/CFT
Zambia	Prohibition and Prevention of Money Laundering Act No 14 of 2001, amended Act No. 44 of 2010; Anti-Terrorism Act No 21 of 2007; Forfeiture of Proceeds of Crime Act No 19 of 2010; Financial Intelligence Centre Act No 46 of 2010; The Public Interest Disclosure (Protection of Whistle-blowers) Act No. 4 of 2010; Mutual Legal Assistance in Criminal Matters Act (MLACMA), 1993; The Plea Negotiations and Agreements Act, No. 20 of 2010; The Anti-Corruption Act, No. 3 of 2012 (replacing the Anti-Corruption Act, No. 38 of 2010).

Source: Researchers’ Own Construction.

5.3.5. Zimbabwe

Table 7 outlines legislation dealing with AML/CFT issues in Zimbabwe. All financial institutions and designated non-financial institutions in Zimbabwe operate within the provisions of the AML/CFT legal framework and guidelines issued by Financial Intelligence Unit of Reserve Bank of Zimbabwe (Maguchu 2018). The FIU derives its powers from the Banking Use Promotion and Suppression of Money Laundering Act (Chapter 24:24) of 2004.

Table 7. Zimbabwe’s Legislation dealing with Anti-Money Laundering.

Country	Legislation Dealing with AML/CFT
Zimbabwe	Banking Use Promotion and Suppression of Money Laundering Act (chapter 24:24) of 2004; Money Laundering and Proceeds of Crime Act (Chapter 9:24) of 2013 amended in 2019; and Suppression of Foreign and International Terrorism Act.

Source: Researchers’ Own Construction.

According to Government of Zimbabwe (2020), the estimated value of money laundered for the period 2004 to 2018 was USD 900 million. Furthermore, Zimbabwe’s money laundering risk was classified as medium by the National Risk Assessment of Zimbabwe. However, own-country assessments could give an impaired conclusion, hence the need to rely on FATF regulatory assessments.

5.3.6. The United Kingdom

The European Union (EU) and the United Kingdom (UK) have also implemented various legislations to counter money laundering threats. Sujee (2016) notes that after the country assessment, the FATF concluded that the UK had the best AML legislative framework, which was compliant with the Vienna and Palermo conventions. Ryder (2012) earlier alluded to the notion that the UK was clearly committed to implementing the best international practices and guidelines on AML. Progressively, the UK has fully embraced a risk-based approach in dealing with money laundering threats (Jones and Knaack 2019; Sujee 2016).

The financial markets in the UK play a significant role in Europe and the whole world, hence posing greater vulnerability and risks. This is due to the magnitude, nature sophistication and location at the epicentre of the world.

The AML/CFT legislative framework in the UK has been broadened to include United Nations and European Union legislative provisions (Sujee 2016; Ryder 2012). Estimates of money laundered annually in the UK are between GBP 23 billion and GBP 75 billion (Financial Service Authority 2013). However, the Home Office Treasury estimated a conservative amount of GBP 10 billion. The AML framework in the UK exceeds the expected international standards (Ngcetane-Vika 2022; Ofoeda 2022; Ryder 2012). Despite having the best legislative AML/CFT regulatory framework, money laundering cases continue to be recorded, even in the UK and the USA. This implies that those launderers continue to devise ways of bypassing the regulatory framework through the use of technology. Hence, regulators need to be proactive.

5.3.7. United States of America

The United States plays a crucial role in the global struggle against money laundering and terrorist funding as the largest economy and most influential national power (Esoimeme 2020). The US has a comprehensive AML/CFT strategy in place that reflects international regulatory standards and applies strict punishments for non-compliance. The US is a member of the Financial Action Task Force (FATF). Therefore, to avoid these penalties, financial businesses need to be aware of the relevant legislation and understand how to comply.

AML/CFT legislation in the USA is underpinned mainly by the Bank Secrecy Act (BSA) and USA Patriot Act. The purpose of the BSA, often referred to as the Currency and Foreign Transactions Reporting Act, is to prevent terrorists from utilising financial institutions to hide or launder their illicit gains. The legislation requires financial institutions to provide documentation to authorities whenever their customers deal with irregular cash exchanges of more than USD 10,000.

Following the terrorist attacks on 11 September 2001, the United States expanded measures to combat ML/TF. By allowing all financial institutions to deploy anti-money laundering (AML) systems, the USA Patriot Act of 2001 modified the BSA. The USA Patriot Act prevents and punishes terrorist crimes, both domestically and abroad, by stepping up law enforcement and improving money laundering controls. Additionally, it promotes the application of research techniques for the prevention of organised crime and drug trafficking in terrorism investigations.

In terms of the regulators, the Financial Crimes Enforcement Network (FinCEN) and Office of Foreign Assets Control (OFAC) are responsible. FinCEN, the primary AML/CFT program of the US Treasury Department, is regulated by one of the most significant agencies in the world: the Financial Intelligence Unit of the United States (FIU). To combat money laundering, terrorism funding, and other financial crimes, FinCEN is in charge of monitoring banks, financial institutions, and other businesses, as well as examining abnormal activities and transfers. Additionally, to exchange information to stop financial crime, FinCEN works with local, state and federal law enforcement agencies.

The Office of Foreign Assets Control (OFAC), which functions similarly to FinCEN in terms of AML/CFT capabilities, is tasked with overseeing and carrying out US economic and trade sanctions. OFAC seeks to prevent blacklisted countries, organisations and individuals from committing financial and related offences.

In the US, there are repercussions for breaking AML rules and regulations ([New York State Department of Financial Services \(DFS\) \(2017\)](#)). According to the guidelines set out by AML authorities, Suspicious Activity Reports (SARs) must be reported in the United States whenever a major or suspicious transaction takes place. Financial institutions in the US are also required to adhere to thorough customer recognition systems to verify each client's real identity and avoid money laundering. However, in more serious circumstances, violations may lead to criminal and civil accusations, fines and jail terms. Each division or site that is determined not to comply with AML requirements may face penalties under the BSA, as well as fines for each day the violation continues. For breaches in client due diligence, the BSA may levy fines ranging from USD10,000 to USD100,000 per day.

5.3.8. European Union

According to [Chico \(2019\)](#) in Europe, money laundering is encompassed in the Council of Europe Directive 91/308/EEC of 1991. Successive amendments have been made in line with FATF recommendations. For instance, the FATF recommendations at the global level especially recommendation 1, which requires that "countries should identify, assess and understand the money laundering and terrorist financing risks for the country" ([FATF 2012](#), p. 11). Article 7 of Directive 2015/849 (or the fourth anti-money laundering directive) transposes this recommendation into an obligation for all EU member states. [Table 8](#) shows the legislation effected in the European Union.

5.3.9. Hong Kong

Hong Kong is required to adopt the most recent FATF recommendations since it is a member of the FATF. [Yim and Philip \(2021\)](#) argued that adhering to global AML/CFT standards is crucial for Hong Kong to remain a major global financial hub. Notably, to incorporate development into the environment, the Anti-Money Laundering and Counter-Terrorist Financing (Financial Institutions) Ordinance (Cap. 615) was renamed the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (Cap. 615) (AMLO), Hong Kong's AML/CFT law, on 1 March 2018 ([Lee 2022](#)). The AMLO (Cap. 615), the Drug

Trafficking (Recovery of Proceeds) Ordinance (Cap. 405), the Organized and Serious Crimes Ordinance (Cap. 455), the United Nations (Anti-Terrorism Measures) Ordinance (Cap. 575), and the United Nations Sanctions Ordinance, and the Weapons of Mass Destruction (Control of Provision of Services) Ordinance are the main pieces of legislation in Hong Kong dealing with AML/CFT issues. The Hong King Monetary Authorities continue to encourage financial institutions to enhance AML/CFT systems by adopting a risk-based approach and applying emerging technologies such as regtech.

Table 8. Legislation in the European Union dealing with AML/CFT.

Group	Legislation Dealing with AML/CFT
European Union	Directive no. 91/308/EEC on the prevention of the use of the financial system for money laundering; Directive no. 2001/97/EC of amending the Directive 91/308/EEC; Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing; Directive 2006/70/EC laying down implementing measures for Directive 2005/60/EC as regards the definition of “politically exposed person” and the technical criteria for simplified customer knowledge procedures and for exceptions to financial activities occasionally or very limited; Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism, adopted in Warsaw on 16 May 2005; 4th AML Directive (EU Directive 2015/849—European Parliament and Council of the European Union 2015—requires ML risk assessment to be performed at three levels: (a) at the supranational level (Directive 2015/849, Art. 6); (b) at the national level (Art. 7); (c) by each obliged entity (Articles 8 and 10–24)

Source: Researcher’s own construction.

5.4. Regulatory Enforcement

Post 2007/8 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 2017). Regulators utilise formal and informal enforcement to deter corrupt behaviour. Enforcement action is dependent on the magnitude of non-compliance. Minor violations require commitment from the senior management on the need to rectify and no public announcement is made thereof. When non-compliance is more severe, this needs to be formalised, publicised and prescribed legally. The safety and soundness of the financial system are affected by AML/CFT non-compliance. There are various enforcements issued out: cease and desist orders; forfeiture orders; and monetary penalties, which are discussed below.

5.4.1. Cease and Desist Order

This is issued when a financial institution fails to establish and maintain an AML programme or correct previously identified deficiencies (ABA 2020; FDIC 2019). Accordingly, this order is issued under these two circumstances. First, failure to maintain the established AML/CFT programme. Second, failure to rectify regulatory deficiencies previously identified. As shown in Table 9, cease-and-desist orders were issued to MUFG Bank, Industrial and Commercial Bank of China, JP Morgan Chase and United Bank for Africa over the period 2008 to 2019. These were issued after deficiencies were noted in the AML/CFT programme and risk management.

These orders were issued mainly by USA regulatory authorities. Larson (2020) argues that the legal counsel of the concerned institution should be aware and appraised of the regulatory effect of being issued with cease-and-desist order. Consequentially, banks can reduce or shift banking operations or restructure the balance sheet. Evidently, the institu-

tion's legal counsel together with AML/CFT team should promote regulatory compliance throughout the organisation.

Table 9. Cease and Desist Orders Issued.

Year	Institution's Name	AML/CFT Deficiency Noted
2019	MUFG Bank—USA	Deficiencies in the BSA/AML programme—training, internal controls, reporting, CDD
2018	Industrial and Commercial Bank of China	Failure to rectify previously noted regulatory shortfalls
2013	JP Morgan Chase	Deficiencies in the BSA/AML programme—training, internal controls, reporting, CDD
2008	United Bank for Africa (New York)	Failure to rectify 2007 regulatory deficiencies and CD order issued in 2007#3. Deficiencies in the BSA/AML programme—training, internal controls, reporting, CDD

Source: [Federal Reserve Bank \(2018\)](#).

5.4.2. Financial Penalties

Financial penalties are levied on repetitive legal infringements or the failure to effect corrective measures ([ABA 2020](#)). The study outlines some of the financial penalties issued hereafter.

(i) United States of America (USA)

[Devoise \(2018\)](#) confirms that more than USD 1.7 billion anti-money laundering regulatory fines were imposed on financial institutions worldwide by mid-2018, which was close to USD 2 billion in 2017. Surprisingly, more than USD 1 billion was from USA regulatory authorities. In the USA, there are several regulatory agencies, such as FinCEN, DoJ and FRB. [Cutter \(2017\)](#) points to the need for regulators in the US to have a single coordinating body on all AML violations and avoid excessively penalising companies.

Regulatory authorities are also obliged to institute personal liability. This was confirmed in the Rabobank case in which an employee was demoted or contract terminated for failure to raise a query on the transaction with the authorities on the inadequacy of the AML/CFT programme. The bank was eventually fined USD 360 million on the related AML/CFT weaknesses ([DoJ 2018](#)).

During the period 2009 to 2014, US Bancorp (USB) failed to provide adequate surveillance on alerts due to insufficient staff ([Devoise 2018](#)). The entity had thresholds proportionate to the transaction risk level. As a result, the USB failed to investigate and detect suspicious transactions. Additionally, the USB filed at least 500 inaccurate and incomplete suspicious transactions based on poor alert mechanisms; eventually, a USD 185 million fine was imposed on the bank ([FinCEN 2018](#)).

(ii) The United Kingdom (UK)

The Financial Conduct Authority (FCA) is the financial regulator. Money laundering through financial institutions undermines the integrity of the financial services sector of the country. UK-based financial institutions need to ensure that the financial system minimises the money laundering risks through proper checks and balances that are conducted routinely ([Financial Conduct Authority 2015](#)).

In 2015, the regulator fined Barclays Bank a penalty amounting to GBP 72.1 million for failing to comply with the CDD principles. The offences were committed from May 2011 to November 2014. The FCA report also verified that Barclays failed to conduct the business operations with due care and diligence to minimise the risk of money laundering. During

the said period of investigation, Barclays Bank facilitated transactions worth GBP 1.88 billion for high-net-worth clients who were classified as politically exposed persons (PEP).

(iii) Namibia

The FIC of Namibia instituted AML/CFT enforcement actions for the period 2016/7. These enforcement actions are publicised in the FIC's Annual Report. This concurs with the transparency stability theory, which requires the publicising of these reports to stakeholders (FATF 2012–2019; Sainah 2015; Tadesse 2006). This also improves the integrity of the financial systems since the banking sector is based on confidence and trust.

5.4.3. Forfeiture Order

The “forfeiture order” is issued as a last resort after exhausting all the other remedies. This order entails removing assets from the institution's operations (FDIC 2019; Gleb 2016). Most countries have this provision in their legislation. For instance, Zambia has Forfeiture of Proceeds of Crime Act 19 of 2010, which caters for civil and criminal seizure of proceeds of crime (Simwayi and Haseed 2011). However, to date, no regulator has exercised this order. This might indicate that regulators fear exercising this order, as this could cause financial instability in the economy. If instituted, this goes against the regulator's mandate of maintaining financial stability and consumer protection, among others.

6. Critique of Global AML/CFT Regulations and Applications

Technology has been designed to bypass existing regulatory frameworks (Rupeika-Apoga and Wendt 2022). The following are the criticisms of the current AML/CFT global regulations as guided by FATF 40 recommendation and from applications of the same.

6.1. Critique by the Application of Global AML/CFT Regulations

6.1.1. Money Laundering Definition

Money laundering is defined as proceeds earned from drug-related offences (Alldridge 2003), while Van Duyne (2003) views money laundering as a process in which the launderers falsify sources of funds as legitimate using the banking system. Additionally, Schneider (2008) posits that money laundering is a criminal activity that includes proceeds from illegal practices. These criminal practices include trade in illegal narcotics, human trafficking, arms trade, fraud and corruption.

The definitions advanced by Schneider (2008), Van Duyne (2003) and Alldridge (2003) concur that money laundering involves legitimising illegally earned proceeds. Schneider's (2008) definition shows the evolving nature of money laundering by including the predicate offences from Van Duyne (2003) and Alldridge (2003) definitions. However, with the passage of time, these definitions fail to capture the electronic and digital avenues used to disguise the original source of funds. These can include international and local money transfers and technology-based means, which are instant and require robust systems controls.

6.1.2. Fintech

Financial technology (fintech) refers to products and services that have become available to the financial services industry because of technological advancements. New York State Department of Financial Services (DFS) (2017) defines fintech as financial innovation derived from technology that delivers new applications, products, services, processes or business models in the financial systems and provision of these services. Fintech denotes firms or companies that offer the latest technologies and apparatuses to the financial services industry (Saksonova and Kuzmina-Merlino 2017). Gomber et al. (2017) view fintech as existing between modern technologies and banking services activities by challenging the existing norms in the banking industry. Puschmann (2017, p. 74) views fintech as “incremental or disruptive innovations in the context of the financial services industry induced by IT developments resulting in new intra- or inter-organisational business models, products and services, organisations, processes and systems”.

The definitions by [Gomber et al. \(2017\)](#), [Saksonova and Kuzmina-Merlino \(2017\)](#), and [Puschmann \(2017\)](#), confirm the existence and incorporation of modern technologies into banking activities. Furthermore, there is no universally accepted definition of fintech, which can be attributed to the evolving nature of the discipline.

6.1.3. Regtech

[Financial Conduct Authority \(2015\)](#), p. 64 defines regulatory technology as “a subset of fintech that focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities.” These are technological solutions that utilise information and technology aimed at addressing regulatory compliance processes and problems ([Johansson et al. 2019](#)). [Butler and Brooks \(2018\)](#) view Regtech as a technology-based solution to several regulatory and compliance problems faced by the financial services industry. Another definition by [Weber and Baisch \(2018\)](#) perceives regtech as the technology-based solutions establishing a relationship between regulator and an intermediary in the scope of system design, compliance and regulation in any industry.

These definitions agree that RegTech is a technology-based solution aimed at addressing regulatory, compliance and system design problems. Thus, [Johansson et al. \(2019\)](#), [Butler and Brooks \(2018\)](#), and [Weber and Baisch \(2018\)](#) argue in their definitions of that effect. [Weber and Baisch \(2018\)](#) further expanded the solutions and understand them as not limited to financial services sector only but pervasive in different organisational spaces, which results in regulatory compliance. The views of [Butler and Brooks \(2018\)](#) can be attributed to the increased regulatory sanctions witnessed after the 2007/8GFC. The definition of the [Financial Conduct Authority \(2015\)](#) further illustrates the notion that RegTech is a subset of FinTech. Therefore, RegTech was developed from FinTech. Thus, RegTech is defined as technology-based solutions that are oriented at regulatory, system design and compliance issues in any sector. This alone demonstrates the complementary nature of addressing regulatory challenges.

6.1.4. Three Stage Process of Money Laundering

Drawbacks of the three-stage process and changes over time have led to the development of new approaches. Critics cite the three-stage process as being too simplified for modern times, as money laundering can happen with no physical or actual money movement (see, for instance, [Naheem 2015, 2018](#); [Choo et al. 2014](#); [Hopton 2009](#)). [Choo et al. \(2014\)](#) argued that the three-stage process fails to take into consideration forms of electronic money being laundered. There have been instances when laundered money was not identified when using the traditional three step process.

For money laundering activities to be effective requires a reliable medium ([Papanicolaou 2015](#)). In order to formalise illegal earnings, money launderers prefer using the financial services sector as a reliable medium ([Sotande 2018](#); [Panda and Leepsa 2017](#)). Evidently, in the USA and Switzerland HSBC cases, money launderers continued to use the formal financial system undetected ([Naheem 2018](#)). In Zimbabwe ([OFAC 2016](#)) and Tanzania ([Mniwasa 2019](#)), foreign AML regulators unearthed money laundering breaches and imposed regulatory penalties. This leaves the financial institution and wider financial system vulnerable to the relentless morphing of laundering practices.

[Hopton \(2009\)](#) posits that money laundering occurs every time a financial transaction or relationship happens, which involves any form of tangible or intangible benefit with origins from criminal activity. This approach is modern and shows that money laundering can occur at any given period, with no money paid or received. Money laundering should be viewed as multi-faceted, complex and ever-evolving ([Naheem 2019](#); [Choo et al. 2014](#)).

6.1.5. Link between Penalty and Violations

[Gleb \(2016\)](#) argued that regulators need to show the link between penalties and AML/CFT violations. The lack of clarity and unpredictable penalties within countries

impede financial sector growth (Zetzsche et al. 2019). Instead, lack of clarity comes from FATF recommendations, which are deemed as advisory rather than enforceable (AL-Rawashdeh 2022; Gomber et al. 2017; Gleb 2016). As a consequence, financial institutions become risk averse to other economic participants, which defeats the financial inclusion regulatory objective.

6.2. Critique by Emerging Trends

6.2.1. Technology Innovations

Technology can result in innovative solutions or disrupt the current financial services and products. Remarkably, if technology leads to innovative solutions, they need to be developed within the present regulatory framework, while if disruption occurs, new development guidelines are needed (Basel Committee on Bank Supervision 2018). The evolving nature and integration of the disciplines influence how to regulate financial transactions of a dubious or suspicious nature. Technological innovations require an interdisciplinary approach to understanding the impact of money laundering (Nejad 2022; Kavuri and Milne 2019). However, innovation and disruption interfere with the offering of services in a heavily regulated financial services sector. By failing to develop effective regulatory measures, money launderers exploit this opportunity by maximising their activities, consequently affecting the integrity and soundness of the banking system.

6.2.2. Technological and Regulatory Gaps

Buttigieg et al. (2019) examined the AML/CFT legal framework for crypto assets in Malta. Malta is considered a small state within the European Union and has the AML/CFT legal framework, which covers virtual assets in the digitalised world as espoused by FATF Recommendation 15. No other country has this legal framework; hence, the model was considered appropriate to serve as the baseline for adoption in the EU. It was further found that the framework addressed regulatory mandates of consumer protection, stability and integrity in the era of digital innovations. The legal framework is seen as a starting point for addressing AML/CFT issues given the rapid pace of financial innovations. However, the technological and regulatory gaps in the implementation of AML/CFT regulations continue to present opportunities for launderers and hinder the effectiveness of regulations. Risk is dynamic and not static. In order to attain regulatory mandates, this should be based on adequate and effective design of data-driven regulations without impeding innovation.

6.2.3. Cyber-Attacks and Data Privacy

Technology lowers compliance costs, while information privacy and security issues remain a threat (Buckley et al. 2020; Butler and Brooks 2018; Chin 2016). Personal information can be misused and stolen by third-party agents. There is a need to minimise this downside of technology with the economy deriving greater benefits. In the face of new products and services, financial institutions still need to verify customers' identities before the commencement of any relationship. Verification may need reliance on third-party service providers, which exposes them to cyber risks and data privacy issues (Mniwasa 2019; Stokes 2012). FATF recommendation 15 states that in outsourcing the technology services, issues of data security and privacy need to be addressed (FATF 2012–2019).

6.2.4. Regulation Paradigm Shift

The paradigm shift from Know Your Customer to Know Your Data shows the movement towards data-based regulations (Perlman and Gurung 2019; Arner et al. 2017; Lootsma 2017). Big data is key in using financial application tools, such as machine learning. Machine learning matches big data to identify any activity or pattern without any human interface. This assists in identifying suspicious transactions. Failure to identify suspicious transactions has been noted as one of the non-compliance reasons for regulatory fines and penalties imposed on banks. Thus, technology could enable financial institutions to have monitoring systems that detect normal and abnormal transaction behaviours. This

aids in reducing the number of false alerts, thereby submitting quality suspicious reports to regulators.

Innovativeness in the financial services industry coupled with financial market transformation for the world warrants redesign and reconceptualisation of financial regulations (Yu et al. 2022; Arner et al. 2017; Brummer 2015). The paradigm shift makes regulations, regulatory bodies and financial services effective in meeting their mandates at an affordable cost (Bains et al. 2022). However, success is based on adequate and effective design of data-driven regulations without impeding innovation and attaining regulatory mandates.

RegTech brings the integration of technology into a bank's risk management processes (Arner et al. 2016, 2017). Most current banking regulations apply to the traditional banking model. However, in the digital innovation era, regulators still require banks to apply the same risk management practices to current digital banking practices. Failure to apply culminates in non-compliance. Fintech is still emerging, evolving and disrupting the financial services industry (Anagnostopoulos 2018; Dong 2017; Brummer 2015). Based on the old regulations, banks are still expected to have sound AML practices. This is detrimental. Studies have opined that in this era of technological innovations, money laundering should be risk based and not rule based (Shust and Victor 2020; ElYacoubi 2020; Naheem 2018; Vasiljeva and Kristina 2016).

7. Conclusions

The study aimed to provide an overview of the global AML/CFT regulations, application and how they should evolve in this dynamic environment. A qualitative enquiry was adopted that involved reviewing FATF recommendations and associated AML/CFT legislation, analysing publicised AML/CFT regulatory enforcements, and related developments.

The study's main findings include the country implementation of the global AML/CFT regulations differed due to political and economic factors, amongst others. The various AML/CFT enforcements done on sampled countries were mainly cease and desist orders and monetary penalties, which were publicised. Forfeiture orders have not been issued. Criticising the global AML/CFT regulations centred on the application of these regulations and emerging trends. These include, among other definitions of money laundering, reference to the three stages of money laundering, link between penalty and violations, technological innovations and regulations paradigm shift, cyber-attacks and data privacy.

The implications of this study indicate that technological innovations have broadened emerging money laundering risks and risks in general to the financial system. Technological innovations can cause financial instability in the financial services sector. Though financial regulation is important for consumer protection, it may also stifle innovation by making it difficult for new players to enter the market. However, the evolving nature and integration of the disciplines influences how to regulate. Hence, regulations should not be static but evolve as well.

The following are the recommendations being proffered. It is our considered view that FATF Recommendations be revised since AML/CFT risk is dynamic in the era of digital innovations. Regulatory enforcement should be risk based and not rule based. Thus, the FATF at the global level should revise the FATF guidelines and be informed by research.

Additionally, AML/CFT regulators need to be pragmatic in responding to the environmental-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. The paradigm shift makes regulations, regulatory bodies and financial services effective in meeting their regulatory mandates.

8. Limitations and Future Research

The study was limited to using documentary analysis, as the financial services sector is associated with privacy and confidentiality issues. Relying on published reports meets the disclosure mandate. Furthermore, money laundering issues were centred on the financial services sector, though designated non-financial institutions are available. Thus,

future studies should focus on designated non-financial institutions. In addition, other studies should revolve around digital innovations and digital economies. Another area includes AML/CFT guidelines for digital currencies and collaborative-based research on the interdisciplinary nature of AML/CFT.

Author Contributions: Conceptualisation, W.G. and A.B.S.; methodology, W.G. and A.B.S.; software, W.G.; validation, W.G. and A.B.S.; formal analysis, W.G.; investigation, W.G.; resources, W.G.; data curation, W.G.; writing—original draft preparation, W.G.; writing—review and editing, A.B.S.; visualisation, W.G.; supervision, A.B.S.; project administration, W.G.; funding acquisition, A.B.S. All authors have read and agreed to the published version of the manuscript.

Funding: The APC was funded by the University of South Africa.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

- ABA. 2020. ABA Legal Technology Survey Report 2020. Available online: https://www.americanbar.org/groups/law_practice/publications/techreport/2020/ (accessed on 23 June 2021).
- Afande, Francis Ofunya, and Mathenge Paul Maina. 2015. Effect of Promotional Mix Elements on Sales Volume of Financial Institutions in Kenya: Case Study of Kenya Post Office Savings Bank. *Journal of Marketing and Consumer Research* 11: 66–67.
- Alldrige, Peter. 2003. *Money Laundering Law: Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime*. New York: Bloomsbury Publishing.
- Al-Nuemat, Ahmed Adnan. 2014. Money laundering and banking secrecy in the Jordanian legislation. *Journal of International Commercial Law and Technology* 9: 117–26. [CrossRef]
- AL-Rawashdeh, Sami Hamdan. 2022. Criminal liability for the crime of money laundering and the regulatory framework for combatting it in Qatari law. *Journal of Legal, Ethical and Regulatory Issues* 25: 1–17.
- Anagnostopoulos, Ioannis. 2018. Fintech and regtech: Impact on regulators and banks. *Journal of Economics and Business* 100: 7–25. [CrossRef]
- Anichebe, Uche. 2020. Combating money laundering in the age of technology and innovation. *Social Science Research Network* 12: 1–35. [CrossRef]
- Arasa, Robert, and Linah Ottichilo. 2015. Determinants of know your customer (KYC) compliance among commercial banks in Kenya. *Journal of Economics and Behavioural Studies* 7: 162–75. [CrossRef]
- Araujo, Ricardo. 2010. An evolutionary game theory approach to combat money laundering. *Journal of Money Laundering Control* 13: 70–78. [CrossRef]
- Armitage, Andrew, and Diane Keeble-Allen. 2008. Undertaking a structured literature review or structuring a literature review: Tales from the field. Paper presented at the 7th European Conference on Research Methodology for Business and Management Studies: ECRM2008, Regent's College, London, UK, June 19–20; p. 35.
- Arner, Douglas Wayne, Janos Nathan Barberis, and Ross P. Buckley. 2016. FinTech, RegTech and the Reconceptualization of Financial Regulation. *Northwestern Journal of International Law & Business*, October 1, Forthcoming. University of Hong Kong Faculty of Law Research Paper No. 2016/035.
- Arner, Douglas Wayne, Janos Nathan Barberis, and Ross P. Buckley. 2017. Fintech, Regtech and the Reconceptualization of Financial Regulation. *NortWestern Journal of International Law and Business* 37: 371–413.
- Arnone, Marco, and Leonardo Borlini. 2010. International anti-money laundering programs: Empirical assessment and issues in criminal regulation. *Journal of Money Laundering Control* 13: 226–71. [CrossRef]
- Bains, Parma, Nobuyaso Sugimoto, and Christopher Wilson. 2022. *BigTech in Financial Services: Regulatory Approaches and Architecture*. FinTech Notes 2022(002). Washington, DC: International Monetary Fund.
- Basel Committee on Bank Supervision. 2018. *Sound Practices: Implications of Fintech Developments for Banks and Banks Supervisors*. Basel: Bank for International Settlements.
- Bofondi, Marcello, and Giorgio Gobbi. 2017. The Big promises of Fintech. In *European Economy Banks, Regulation, and the Real Sector 2017*. Torino: Associazione Centro Studi Luca d'Agliano, pp. 107–20.
- Brummer, Chris. 2015. Disruptive Technology and Securities Regulation. *Fordham Law Review* 84: 84–95. [CrossRef]
- Buckley, Ross, Douglas Arner, Dirk Zetzsche, and Rolf Weber. 2020. The road to RegTech: The (astonishing) example of the European Union. *Journal of Banking Regulation* 21: 26–36. [CrossRef]
- Butler, Tom, and Robert Brooks. 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* 11: 19–33.
- Buttigieg, Christopher P., Christos Efthymiopoulos, Abigail Attard, and Samantha Cuyle. 2019. Anti-money laundering regulation of crypto assets in Europe's smallest member state. *Law and Financial Markets Review* 13: 211–27. [CrossRef]
- Chico, Oana. 2019. Money laundering Internationally. *Perspectives of Law and Public Administration* 8: 74–78.

- Chin, Ian. 2016. FinTech and disruptive business models in financial products, intermediation and markets: Policy implications for financial regulations. *Journal of Technology and Law* 21: 6–20.
- Choo, Huang Ching, Mira Susanti Amirrudin, Nur Adura Ahmad Noruddin, and Rohana Othman. 2014. Anti-Money Laundering and its effectiveness. *Malaysian Accounting Review* 13: 109–24.
- Clarke, Andrew Emerson. 2021. Is there a commendable regime for combatting money laundering in international business transactions? *Journal of Money Laundering Control* 24: 163–76. [CrossRef]
- Collin, Matthew. 2020. Illicit financial flows: Concepts, measurement, and evidence. *The World Bank Research Observer* 35: 44–86. [CrossRef]
- Cooper, Randolph, and Zmud Robert. 1990. Information Technology Implementation Research: A Technological Diffusion Approach. *Management Science* 36: 123–39. [CrossRef]
- Cutter, Henry. 2017. Department of Justice targets duplicate penalties through increased coordination. *Wall Street Journal* 3: 10.
- De Koker, Louis. 2022. Editorial: Regulatory impact assessment: Towards a better approach for the FATF. *Journal of Money Laundering Control* 25: 265–67. [CrossRef]
- De Koker, Louis, and Mark Turkington. 2016. *Transnational Organised Crime and the Anti-Money Laundering Regime*. Edited by Hauck Peter and Peterke Simon. Oxford: International Law and Transnational Organised Crime, Oxford University Press, pp. 241–63.
- Deboise. 2018. *2018 Mid-Year Anti-Money Laundering Review and Outlook*. New York: Deboise & Plimpton LLP.
- Demetis, Dionysios. 2010. *Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach*. Cheltenham: Edward Elgar Publishing.
- Dobrowolski, Zbysław, and Łukasz Sułkowski. 2020. Public ethnocentrism: A cognitive orientation and preventive measures. *Journal of International Studies* 13: 178–90. [CrossRef]
- DoJ. 2018. *Rabobank Pleads Guilty and Agree to Pay USD360 Million*; Washington, DC: US Department of Justice.
- Dong, He. 2017. *Fintech and Cross Border Payments*. New York: Central Bank Summit.
- Dumitrache, Ana Alina, and Georgeta Modiga. 2011. New trends and perspectives in the money laundering process. *Challenges of the Knowledge Society Law* 1: 50–57.
- ELYacoubi, Dina. 2020. Challenges in customer due diligence for banks in the UAE. *Journal of Money Laundering Control* 23: 527–39. [CrossRef]
- Esoimeme, Eric Ehi. 2020. Identifying and reducing the money laundering risks posed by individuals who been unknowingly recruited as money mules. *Journal of Money Laundering Control* 24: 201–12. [CrossRef]
- European Commission. 2016. ECB Ends Production and Issuance of €500 Banknote. Available online: <https://www.ecb.europa.eu/press/pr/date/2016/html/pr160504.en.html> (accessed on 12 May 2020).
- FATF. 2012. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. The FATF Recommendations. Paris: Financial Action Task Force—Organization for Economic Cooperation and Development. Available online: http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf (accessed on 18 March 2020).
- FATF. 2012–2019. *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*. Paris: FATF.
- FATF. 2021. High-Level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards. Paris. Available online: www.fatf-gafi.org/media/fatf/documents/Unintended-Consequences.pdf (accessed on 26 December 2022).
- FDIC. 2019. Enforcement Decisions and Orders. Available online: <https://www.fdic.gov/news/press-releases/2019/pr19114.html> (accessed on 18 October 2020).
- Federal Reserve Bank. 2018. *Joint Statement on Innovative Efforts to Combat Money Laundering and Terrorist Financing*. New York: Federal Reserve Bank.
- Filipkowski, Wojciech. 2008. Cyber Laundering: An Analysis of Typology and Techniques. *International Journal of Criminal Justice Sciences* 3: 15–27.
- Financial Conduct Authority. 2015. *FCA Fines Barclays £72 Million for Poor Handling of Financial Crime Risks*. London: Financial Conduct Authority.
- Financial Service Authority. 2013. *FCA Fines Guaranty Trust Bank (UK) Ltd £525,000 for Failures in Its Anti-Money Laundering Controls*. London: Financial Conduct Authority.
- FinCEN. 2018. *FinCEN Penalizes US Bank National Association for Anti-Money Laundering Laws Violations*. Vienna: FinCEN.
- Gaviyau, William, and Athenia Bongani Sibindi. 2023. Customer Due Diligence in the FinTech Era: A Bibliometric Analysis. *Risks* 11: 11. [CrossRef]
- GIABA. 2015. *Seventh Follow Up Report on Nigeria Mutual Evaluation*. Dakar: GIABA.
- Gleb, Alan. 2016. *Balancing Financial Integrity with Financial Inclusion: The Risk based approach to “Know Your Customer”*. CDG Policy Paper 74. Washington, DC: Centre for Global Development.
- Gomber, Peter, Jascha-Alexander Koch, and Michael Siering. 2017. Digital Finance and FinTech: Current research and future research directions. *Journal of Business Economics* 87: 537–80. [CrossRef]
- Government of Botswana. 2018. *Anti-Money Laundering Annual Report*; Gaborone: Government of Botswana.
- Government of Zimbabwe. 2020. *Money Laundering and Proceeds of Crime (Amendment) Act, 2019*; Harare: Government of Zimbabwe.
- Groepe, Francois. 2017. Regulatory responses to Fintech development. Paper presented at the Joburg, Strate GIBS Fintech Innovation Conference 2017, Johannesburg, Germany, August 22.
- Held, Micheal. 2019. *The First Line of Defence and Financial Crime*. New York: The First Line of Defence Summit.

- Hill, John. 2018. *Fintech and the Remaking of Financial Institutions*. Cambridge: Academic Press.
- Hopton, Doug. 2009. *Money laundering: A concise guide for all business*. Burlington and Aldershot: Gower Publishing, Ltd.
- Johansson, Ellinor, Sutinen Julius, Valter Lang, Minna Martikainen, and Othar Lehner. 2019. Regtech—a necessary tool to keep up with compliance and regulatory changes. *ACRN Journal of Finance and Risk Perspectives, Special Issue Digital Accounting* 8: 71–85.
- Jones, Emily, and Peter Knaack. 2019. Global financial regulation: Shortcomings and reform options. *Global Policy* 10: 193–206. [CrossRef]
- Kaur, Sharanpreet, and Navneet Kaur Sandhu. 2022. Novel Technique of Anti-Money Laundering Using Deep Learning. *Journal of Emerging Technologies and Innovative Research (JETIR)* 9: 532–37.
- Kavuri, Anil Savio, and Alistair Milne. 2019. *FinTech and the Future of Financial Services: What Are the Research Gaps?* CAMA Working Paper 18/2019. Canberra: Australia National University.
- Kirakul, Sasin, Yong Jeffery, and Zamil Raihan. 2021. *The Universe of Supervisory Mandates—Total Eclipse of the Core?* FSI (30). Basel: Bank for International Settlements.
- Larson, Benjamin James. 2020. False Positive Reduction in Credit Card Fraud Prediction: An Evaluation of Machine Learning Methodology on Imbalanced Data. Ph.D. dissertation, Capitol Technology University, Laurel, MD, USA.
- Lee, Emily. 2022. Technology-driven solutions to banks' de-risking practices in Hong Kong: FinTech and blockchain-based smart contracts for financial inclusion. *Common Law World Review* 51: 83–108. [CrossRef]
- Littrell, Charles. 2022. Biases in National Anti-Money Laundering Risk Assessments. January 21. Available online: <https://ssrn.com/abstract=4137532> (accessed on 30 December 2022).
- Lootsma, Yvonne. 2017. Blockchain as the newest regtech application—The opportunity to reduce the burden of kyc for financial institutions. *Banking & Financial Services Policy Report* 36: 16–21.
- Magarura, Dennis. 2013. Credit Reference Bureau Services and Loan Performance in Microfinance Deposit Taking Institutions in Uganda. Ph.D. dissertation, Uganda Martyrs University, Nkozi, Uganda.
- Maguchu, Prosper Simbarashe. 2018. The law is just the law: Analysing the definition of corruption in Zimbabwe. *Journal of Financial Crime* 25: 354–61. [CrossRef]
- Masciandaro, Donato. 1999. Money Laundering: The Economics of Regulation. *European Journal of Law and Economics* 7: 225–40. [CrossRef]
- Mathuva, David, Sammy Kiragu, and Dulacha Barako. 2020. The determinants of corporate disclosures of anti-money laundering initiatives by Kenyan commercial banks. *Journal of Money Laundering Control* 23: 609–35. [CrossRef]
- Meiryani, Meiryani, Soepriyanto Gatot, and Audrelia Jessica. 2022. Effectiveness of regulatory technology implementation in Indonesian banking sector to prevent money laundering and terrorist financing. *Journal of Money Laundering Control* 26: 892–908. [CrossRef]
- Mniwasa, Eugene. 2019. Money laundering control in Tanzania: Did the bank gatekeepers fail to discharge their obligations? *Journal of Money Laundering Control* 22: 796–835. [CrossRef]
- Mohr, Philip, and Fourie Lewis. 2008. *Economics for South African Students*, 4th ed. Pretoria: Van Schaik.
- Moiseienko, Anton. 2022. Does international law prohibit the facilitation of money laundering? *Leiden Journal of International Law* 36: 109–32. [CrossRef]
- Mynhardt, Ronald Henry, and Marx Johan. 2013. Anti-Money Laundering Recommendations for Cash based economies in West Africa. *Corporate Ownership and Control* 11: 24–32. [CrossRef]
- Naheem, Mohammed Ahmad. 2015. Trade based money laundering: Towards a working definition for the banking sector. *Journal of Money Laundering Control* 18: 513–24. [CrossRef]
- Naheem, Mohammed Ahmad. 2018. TBML suspicious activity reports—A financial intelligence unit perspective. *Journal of Financial Crime* 25: 721–33. [CrossRef]
- Naheem, Mohammed Ahmad. 2019. Anti-money laundering/trade-based money laundering risk assessment strategies—action or re-action focused? *Journal of Money Laundering Control* 22: 721–33. [CrossRef]
- Namibia Financial Intelligence Centre. 2017. *Annual Report 2016/2017*. Windhoek: Financial Intelligence Centre.
- Nejad, Mohammad. 2022. Research on financial innovations: An interdisciplinary review. *International Journal of Bank Marketing* 40: 578–612. [CrossRef]
- New York State Department of Financial Services (DFS). 2017. DFS Fines Deutsche Bank \$425 Million for Russian Mirror-Trading Scheme. January 25. Available online: <https://www.dfs.ny.gov/about/press/pr1701301.htm> (accessed on 16 January 2020).
- Ngcetane-Vika, Thelela. 2022. Comparative Analysis of Anti-money Laundering (AML) and Counter Terrorist Financing (CTF) Regimes in the UK and USA. *AfricArXiv*, May 31. [CrossRef]
- OECD. 2022. *Regulatory Impact Assessment*. Paris: OECD. Available online: www.oecd.org/regreform/regulatory-policy/ria.htm (accessed on 26 December 2022).
- OFAC. 2016. *Enforcement Information*; New York: Office of Foreign Assets and Control, USA Department of Treasury Office.
- Ofoeda, Isaac. 2022. Anti-money laundering regulations and financial inclusion: Empirical evidence across the globe. *Journal of Financial Regulation and Compliance*, forthcoming.
- Panda, Brahmadev, and Nabaghan Madhabika Leepsa. 2017. Agency theory: Review of theory and evidence on problems and perspectives. *Indian Journal of Corporate Governance* 10: 74–95. [CrossRef]

- Papanicolaou, George. 2015. One Stop Brokers. Available online: <https://www.onestopbrokers.com/2015/01/12/stages-money-laundering/> (accessed on 14 September 2018).
- Perlman, Leon, and Nora Gurung. 2019. Focus Note: The Use of eKYC for Customer Identity and Verification and AML. *Social Science Research Network*, 1–28. [CrossRef]
- Puschmann, Thomas. 2017. Fintech. *Business & Information Systems Engineering* 59: 69–76.
- Rupeika-Apoga, Ramona, and Stefan Wendt. 2022. FinTech Development and Regulatory Scrutiny: A Contradiction? The Case of Latvia. *Risks* 10: 167. [CrossRef]
- Ryder, Nicholas. 2012. *Money Laundering-an Endless Cycle?: A Comparative Analysis of the Anti-money Laundering Policies in the United States of America, the United Kingdom, Australia and Canada*. Abingdon-on-Thames: Routledge.
- Sainah, Ruth C. 2015. The Effect of Anti Money Laundering Risk Assessment on the Financial Performance of Commercial Banks in Kenya. Ph.D. dissertation, University of Nairobi, Nairobi, Kenya.
- Saksonova, Svetlana, and Irina Kuzmina-Merlino. 2017. Fintech as financial innovation—The possibilities and problems of implementation. *European Research Studies* 20: 961–73. [CrossRef]
- Schneider, Friedrich. 2008. Money Laundering and Financial Means of Organized Crime: Some Preliminary Empirical Findings (May 2008). Paolo Baffi Centre Research Paper No. 2008-17. Available online: <https://ssrn.com/abstract=1136149> (accessed on 1 May 2023). [CrossRef]
- Sherman, Lawrence. 1993. Defiance, deterrence, and irrelevance: A theory of the criminal sanction. *Journal of Research in Crime and Delinquency* 30: 445–73. [CrossRef]
- Shust, Pavel, and Dostov Victor. 2020. Implementing Innovative Customer Due Diligence: Proposal for Universal Model. *Journal of Money Laundering Control* 23: 871–84. [CrossRef]
- Sileshi, Belay. 2022. Effectiveness of Anti-money Laundering Preventive Measures in Ethiopia: Case Study on Commercial Banks and Financial Intelligence Center. Ph.D. dissertation, St. Mary's University, San Antonio, TX, USA.
- Simwayi, Musonda, and Muhammed Haseed. 2011. The role of financial intelligence units in combating money laundering: A comparative analysis of Zambia, Zimbabwe and Malawi. *Journal of Money Laundering Control* 15: 112–34. [CrossRef]
- Solin, Marina, and Andrew Zerzan. 2010. *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks*. London: The GSM Association.
- Sotande, Emmanuel. 2018. The regime against money laundering: A call for scientific modelling. *Journal of Money Laundering Control* 21: 584–93. [CrossRef]
- Stessens, Guy. 2000. *Money Laundering: A New International Law Enforcement Model (Cambridge Studies in International and Comparative Law)*. Cambridge: Cambridge University Press.
- Stokes, Robert. 2012. Virtual money laundering: The case of Bitcoin and the Linden dollar. *Information & Communications Technology Law* 21: 221–36.
- Sujee, Zain Jadewin. 2016. A Study of the Anti-Money Laundering Framework in South Africa and the United Kingdom, Pretoria, South Africa. Ph.D. thesis, Univeristy of Pretoria, Pretoria, South Africa.
- Sultan, Nasir, and Norazida Mohamed. 2022. Financial intelligence unit of Pakistan: An evaluation of its performance and role in combating money laundering and terrorist financing. *Journal of Money Laundering Control* 26: 862–76. [CrossRef]
- Suntura Clavijo, Joel Harry. 2020. Customer identification in currency exchange companies as per FATF recommendations. *Journal of Money Laundering Control* 23: 96–102. [CrossRef]
- Tadesse, Solomon. 2006. The economic value of regulated disclosure: Evidence from the banking sector. *Journal of Accounting and Public Policy* 25: 32–70. [CrossRef]
- Teichmann, Fabian Maximilian Johannes, and Chiara Wittmann. 2022. Money laundering in the United Arab Emirates: The risks and the reality. *Journal of Money Laundering Control* 26: 709–18. [CrossRef]
- Trajkovski, Goce, and Blagoja Nanevski. 2019. Customer Due Diligence—Focal Point of Anti-Money Laundering Process. *Journal of Sustainable Development* 5.
- Van Duyne, Petrus C. 2003. Money laundering policy: Fears and facts. In *Criminal Finances and Organising Crime in Europe*. Nijmegen: Wolf Legal, pp. 67–104.
- Vasiljeva, Tatjana, and Lukanova Kristina. 2016. Commercial Banks and Fintech Companies in the Digital Transformation: Challenges for the future. *Journal of Business Management*, 25–33.
- Weber, Rolf, and Rainer Baisch. 2018. FinTech-eligible safeguards to foster the regulatory framework. *Journal of Financial Regulation and Compliance* 33: 335–50.
- Whisker, James, and Mark Eshwar Lokanan. 2019. Anti-money laundering and counter terrorist financing threats posed by mobile money. *Journal of Money Laundering Control* 22: 158–72. [CrossRef]
- Yim, Foster Hong-Cheuk, and Lee Ian Philip. 2021. Updates on Hong Kong's anti-money laundering laws 2020. *Journal of Money Laundering Control* 24: 3–9. [CrossRef]
- Yu, Poshan, Ruixin Gong, and Michael Sampat. 2022. Blockchain Technology in China's Digital Economy: Balancing Regulation and Innovation. In *Regulatory Aspects of Artificial Intelligence on Blockchain*. Hershey: IGI Global, pp. 132–57.

Yuen, Aurthur. 2018. *Regetch in the Smart Banking Era—A Supervisor’s Perspective*. Hong Kong: HKIB Annual Banking Conference.

Zetzsche, Dirk, Douglas Arner, Ross Buckley, and Rolf Weber. 2019. The future of datadriven finance and RegTech: Lessons from EU big bang II. Available online: <https://ssrn.com/abstract=3359399> (accessed on 1 May 2023).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.