**Mitigating Money Laundering in Sri Lanka: Evaluating Legal Frameworks, Enforcement Challenges and International Compliance**

**ABSTRACT**

The criminal practice of money laundering (ML) is increasingly interconnected across various jurisdictions due to its transnational nature. ML poses a significant threat to global financial systems, necessitating coordinated efforts at both national and international levels to combat its adverse effects. Law enforcement agencies within anti-money laundering (AML) frameworks face significant challenges in addressing this issue, though it cannot be entirely eradicated. It is crucial to comprehensively understand the fundamental principles of ML as a step towards developing effective AML standards. This research examines the ramifications of ML within the financial sector and the proactive measures implemented by financial institutions to mitigate the infiltration of illegal funds, ensuring the provision of secure and reliable financial services to the nation, while safeguarding the long-term sustainability of the financial sector. The study emphasizes the significance of combating ML as a pervasive issue and focuses on Sri Lanka's experience in addressing ML, examining the effectiveness of its legal frameworks, enforcement mechanisms and compliance with international standards. Despite enacting laws such as the Prevention of Money Laundering Act, Financial Transaction Reporting Act and establishing a Financial Intelligence Unit, Sri Lanka continues to face challenges due to coordination difficulties, political interference and ineffective implementation. This paper analyzes these challenges and explores efforts to enhance the powers of the FIU to strengthen the country's AML regime. Furthermore, it highlights the necessity for effective international cooperation and the establishment of strong local AML systems that adhere to global standards. Methodologically, this research adopts a doctrinal approach to examine and analyze international perspectives and global initiatives to combat ML and evaluates the adherence of Sri Lankan entities to these standards, highlighting areas for improvement. Through a comprehensive analysis of Sri Lanka's AML efforts, this research aims to provide insights into effective strategies for combating money laundering in similar contexts globally.

**Keywords**: Money Laundering, Financial Institutions, Legal Frameworks, Enforcement Challenges, International Compliance

1. **Introduction**

Money laundering (ML) encompasses a series of activities designed to disguise the illicit origins of funds acquired through criminal activities like drug trafficking, corruption, fraud and terrorism. These activities progress through a sophisticated and discreet process of disguising the ill-gotten money and the culprits which processed in three distinct stages: placement, layering and integration. Initially, illicit funds enter the financial system through various channels such as cash deposits, wire transfers or investments during the placement phase. Subsequently, in the layering stage, funds undergo a complex web of transactions and transfers across multiple accounts to obscure their source and ownership. Finally, laundered funds are reintroduced into the legitimate economy through apparently lawful avenues in the integration phase, effectively masking their illicit origins.

Money Laundering (ML) refers to the illegitimate use of banking and other associated facilities and channels for the concealment of unlawfully acquired wealth by those with malicious intent. The global ramifications of this malfeasance have necessitated an international response, leading to the development of a coordinated strategy to mitigate its adverse effects. This is primarily due to the fact that ML is not confined to a single country or region and is viewed as a global menace with devastating multifaceted repercussions, making detection an arduous task. Technological advancements driven by globalization have intensified the impact of ML, particularly in nations with deficient financial regulatory systems and lenient regulations. Consequently, the integrity of financial institutions in such nations is severely compromised. The repercussions of this negative phenomenon of ML have impeded the overall financial and economic stability and viability of the affected nations and Sri Lanka is no exception. In an era where expediency is paramount in financial transactions, those engaging in ML circumvent controls, compromising the security of economic and financial infrastructures. To counteract the threat posed by ML and to ensure the economic health and financial well-being of the nation, a stringent and effective legal framework that promotes sustainable economic practices and includes effective checks and balances is essential. Sri Lanka has become a haven and hub for those seeking to avoid legal consequences and concealing ill-gotten wealth, due to its lenient financial regulations.

Sri Lanka was one of the leading South Asian nations in enacting legislation to combat ML and countering the financing of terrorism (CFT). The country enacted the Prevention of Money Laundering Act No. 5 of 2006 as amended by Act No. 40 of 2011(PMLA), Convention on the Suppression of Terrorist Financing Act, No. 25 of 2005 (CSTFA) as amended by Act Nos. 41 of 2011 and 3 of 2013 and the Financial Transaction Reporting Act No. 6 of 2006 (FTRA), which are considered as primary AML laws to address these concerns. In addition, the Central Bank of Sri Lanka (CBSL) established the Financial Intelligence Unit of Sri Lanka (FIU) in 2006. The FIU plays a pivotal role in coordinating efforts with various stakeholders, including the Police, Attorney General's Department, Judiciary, Bribery Commission etc. In addition to the above laws, other legislation indirectly related to combating ML, along with Extraordinary Gazettes issued by the government from time to time, also exist.

Despite these proactive measures, Sri Lanka continues to face challenges in establishing an effective system of safeguards due to coordination difficulties, political interference, ineffective implementation, lax controls in the Prison Department and primarily due to its archaic enforcement mechanisms (Patabendige, 2023 [1]). The non-compliance with international standards by a number of entities has also been a contributory factor in aggravating of this situation. As a response, efforts have been made to enhance the powers of the FIU to address these issues effectively. Consequently, it is crucial to assess the adverse impacts of ML on the Sri Lankan economy. To prevent any perception that Sri Lanka facilitates ML, the country has taken significant strides in various areas, such as imposing extended prison sentences, confiscating assets and implementing other legal measures.

Prior to 2019, Sri Lanka was considered to have inadequate measures for combatting ML. This was evidenced by its classification as a high-risk jurisdiction by the Financial Action Task Force (FATF). FATF has been instrumental in strengthening global AML initiatives by establishing international standards and creating a thorough framework to address and combat ML and TF worldwide. The FATF provides recommendations for countries to implement within their legal, regulatory and operational frameworks. Due to significant shortcomings in Sri Lanka's anti-ML measures, it was included in the FATF's "grey list". Although the grey listing is a warning measure, it is commonly perceived that nations on this list are regarded as high-risk countries. Being on the grey list often leads to blacklisting by various jurisdictions. After Sri Lanka was grey-listed for the second time, subsequently the European Union decided to include the country in its blacklist (EconomyNext, 2023 [2]).

Following a review initiated by the FATF in October 2016, Sri Lanka's progress in addressing strategic AML/CFT deficiencies was acknowledged during the FATF's plenary in Paris. As a result of these advancements, Sri Lanka is no longer subject to FATF monitoring, indicating a notable shift in its compliance status. The latest Mutual Evaluation Report, published in 2021, further solidified this progress, finding Sri Lanka compliant with 7 and largely compliant with 25 of the FATF 40 Recommendations, reflecting a marked improvement in its AML/CFT effectiveness (Central Bank of Sri Lanka, n.d.[3]). ‘Although the European Union’s decision to decline EU blacklist, which encompassed Sri Lanka, provides temporary relief for Sri Lanka, it highlights the importance of the country upgrading its Anti-Money Laundering and Counter Financing of Terrorism (AML/CTF frameworks to meet international standards. This is crucial for Sri Lanka's goal of becoming a prominent financial center in the region’(Gunawardena & Maharoof, 2019 [4]). Sri Lanka must maintain enhanced follow-up procedures and report progress regularly to the Asia/Pacific Group on ML (APG) to strengthen its AML/CFT measures (FATF, 2020 [5]).

‘‘The introduction of Sri Lanka's National Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT) Policy (National Policy) for 2023 – 2028 (National Policy) signifies a critical step in addressing the pressing concerns surrounding the prevention and combatting of ML and TF within the country. This comprehensive framework has been meticulously developed to mitigate the inherent threats, vulnerabilities and risks associated with ML and TF, emphasizing the necessity for domestic mechanisms to ensure effective risk minimization. The National Policy has been formulated based on the insights garnered from Sri Lanka's National Money Laundering and Terrorist Financing Risk Assessment (NRA for 2021/2022) on ML and TF conducted during 2021/2022, aiming to rectify significant structural vulnerabilities and strategic deficiencies within the nation's AML/CFT regime, all in accordance with the FATF Recommendation 2 (Ministry of Justice, 2023 [6])This assessment, coordinated by the FIU of Sri Lanka, involved collaboration among significant government and private sector stakeholders and took place over an 18-month period from July 2021 to December 2022. The analysis focused on key sectors such as banking, non-banking financial institutions and designated non-financial businesses and professions (DNFBPs) to evaluate Sri Lanka's AML measures. It aimed to assess the alignment of these measures with the identified threats and risks. The findings indicate that both the overall ML threat and vulnerability in Sri Lanka are rated as medium, with a similar assessment for terrorist financing (TF) risks.

Further, the NRA for 2021/2022 identified significant gaps in Sri Lanka's AML/CFT regime, including deficiencies in the legal and institutional framework, low levels of investigations and prosecutions, lack of data on ML and TF activities, poor inter-agency coordination and inadequate resources and expertise. Additionally, there is a need for centralized legal frameworks and regulatory authorities in sectors like real estate and casinos to address vulnerabilities to illicit financial activities. Addressing these issues is crucial for strengthening Sri Lanka's AML/CFT efforts and mitigating risks associated with ML/TF (at page 11 [6]).

The IMF has emphasized the necessity for Sri Lanka to adhere to the latest international AML/CFT compliance obligations as part of the conditions for its $3 billion loan. Failure to address potential ML and TF vulnerabilities could place Sri Lanka at risk of being Grey Listed. In February 2010, Sri Lanka was first added to the Grey List after Mahinda Rajapaksa's election victory following the end of a 26-year war. As the government partially complied with AML obligations, it was delisted in June 2013. However, the country was grey-listed again in November 2017 as being vulnerable to ML and removed from the list in October 2019.

To mitigate these risks, Sri Lanka must take decisive action, including enacting new legislation to align with AML/CFT standards before the upcoming evaluation in March 2026. With Sri Lanka having already been Grey Listed twice in the past 14 years, the stakes are high for both the domestic and global financial systems as well as for peace and development. Non-compliance will lead to Sri Lanka being identified as a country with strategic deficiencies in its AML/CFT framework, potentially resulting in Grey or Blacklisting [5]. Such a listing could economically isolate Sri Lanka from developed countries, harming its economy (Ferwerda, Deleanu, & Unger, 2019 [7]).

1. **DEFINITION AND SCOPE**

The study aims to analyze the impact of ML on the financial sector in Sri Lanka and evaluate the measures implemented by banks and financial institutions to prevent the illegal use of funds within the system. The study assesses the importance of combating ML and analyzes the responses of both domestic and international regulatory bodies. Furthermore, the research provides an analysis of the legal frameworks, enforcement mechanisms and compliance with international standards on ML in Sri Lanka, exploring their implications on the country's financial arena. This research also analyzes the challenges and initiatives to empower the FIU to strengthen the country's anti-money laundering AML regime. Furthermore, it analyzes international perspectives and global initiatives to combat ML and evaluates the adherence of Sri Lankan entities to these standards, highlighting areas for improvement and the legal capacity to adapt to emerging trends.

* 1. **Hypothesis**

Legal frameworks and international compliance measures in Sri Lanka have significantly contributed to combating ML. By further strengthening enforcement mechanisms and strict adherence to international cooperation and compliance measures, Sri Lanka can effectively combat ML activities and **mitigate associated risks.** This approach will help to improve the country's AML regimes to better address emerging ML trends.

**2.2 Limitations**

This research acknowledges the significant connection between ML and terrorist financing (TF), however, it specifically focuses on ML in Sri Lanka. The study aims to conduct a thorough and detailed analysis of the legal frameworks, challenges in enforcement and compliance issues related to ML in Sri Lanka. By focusing solely on ML, the research provides a detailed examination of the complexities involved, offering insights and recommendations. Given the multifaceted nature of ML, addressing both ML and TF within a single research study may result in oversimplification or overlooking important aspects of either phenomenon. This study only focuses on a legal analysis of legislation and a critical examination of the enforcement mechanisms employed by authorities responsible for anti-money laundering (AML). This will contribute to the development of more effective policy responses and regulatory frameworks in Sri Lanka.

1. **MATERIALS AND METHODS**

The research methodology employed in this study is a mixed approach of the ‘black letter’ and a ‘socio-legal’ approach. This is a doctrinal and analytical research study using both primary and secondary sources to ensure a comprehensive and reliable analysis. Primary data consists of domestic legislation, case laws and judgements and law reform documents in Sri Lanka while secondary sources such as scholarly literature, academic writings and international standard-setting documents were also utilized to facilitate a thorough examination of the various aspects covered in the research. This is a qualitative study that analyzes both primary and secondary data related to AML laws and regulations in Sri Lanka and globally.

1. **DISCUSSION**

**4.1 What is Money Laundering?**

The nature of ML evolves over time, leading to ambiguous forms that challenge the establishment of a complete definition. This is particularly relevant for contemporary innovations such as cryptocurrencies and blockchain technology, which are revolutionizing electronic banking. These advancements often operate in an invisible manner and remain largely unregulated, making it challenging to impose penalties.

ML is a process of converting cash, funds or property derived from criminal activities to give it a legitimate appearance. It is a process to clean ‘dirty’ money in order to disguise its criminal origin’ (Bank Negara Malaysia, n.d. [8]). ML is the systematic process of making illegally obtained funds appears legitimate. It is a form of "predicate offence," which refers to initial criminal acts that subsequently generate further criminal activity. These predicate offences encompass a range of unlawful activities, including drug trafficking, smuggling, extortion, tax evasion, capital market trade manipulation and ransom. This is not an exhaustive list, as there are other crimes globally classified as illegal. The technical dimension of ML involves the complex process of transforming illegally acquired wealth into wealth with a legitimate origin. In simpler terms, ML is money earned through unlawful means to appear as if it was obtained through legal means.

The allure of accumulating wealth through illegal means is undoubtedly strong, which creates a significant challenge for the lawful banking and financial systems of Sri Lanka in their fight against ML (Ceylon Today, 2023 [9]). The gains and profits derived from such activities are undoubtedly the product of criminal activities and persons involved in such initial transactions seek avenues to validate the legitimacy of their ill-gotten gains and integrate them into the larger financial system. Of the three phases of money laundering, the third stage is the most crucial and pivotal, making detection nearly impossible. At this point, money launderers have successfully integrated their illicit funds into the financial system. The illicit money has been "sanitized," making it appear as though it was obtained through legitimate means (Levi & Reuter, 1997 [10]). The inherent weaknesses within Sri Lanka's banking system have been exploited to conceal the criminal origins of these proceeds (Heart, 2019 [11]). A considerable portion of such unlawfully obtained resources is directed towards the maintenance of the lavish lifestyles of the perpetrators, including the purchase of luxury goods, such as high-end cars, boats, jets, real estate and artwork. In essence, the process of legitimizing unlawfully acquired funds is recognized as ML, facilitated by exploiting vulnerabilities present in the banking system.

**4.2 Impact of money laundering on the Financial Sector**

The banking system is a vital component of a country's economy, facilitating financial transactions and operations. However, money launderers have exploited this essential infrastructure to carry out illicit activities. They use banks to deposit, withdraw and transfer money and banks, who are entrusted with such tasks, become unwitting facilitators in this process (Fundanga, 2003) and (Thommandru & Chakka, n.d.[12]). The banking system's extensive national and international reach makes it an attractive target for illegal transactions.

Studies have shown that money launderers often use both national and international financial institutions, including banks, non-banking entities and equity markets, to launder illegally obtained money. Developing countries, in particular, are being used as vehicles during the initial stages of "placement" and "layering" in the ML process. The financial and economic systems of these countries have inherent vulnerabilities that allow for the circulation of illegal funds with ease. As a result, regulatory and enforcement agencies struggle to trace the origins of such funds, which makes it easy to integrate the tainted money into the legitimate financial system (IMF, 2023 [13]). This poses significant challenges in combating ML activities.

In the post–conflict era, with the end of a thirty-year civil war, Sri Lanka has witnessed rapid economic development.  As a result, the necessity for more foreign capital inflow through the banking system has been recognized as beneficial. However, this necessity can be exploited by money launderers to channel and invest unlawfully obtained money. The influx of foreign capital could potentially be manipulated by money launderers to advance their objectives of depositing and investing unlawfully acquired wealth (Brada, Drabek, & Perez, n.d. [14]). Moreover, with the increase in economic development projects and money circulation, the risk of crimes such as bribery, theft, misappropriation, fraud and corruption may escalate, posing a threat to the overall economy (Bhargava & Bolongaita, 2004 [15]).

Another major reason behind ML occurring in financial institutions is the weak internal controls of banks, financial institutions, and other entities, particularly their inability to conduct Customer Due Diligence (CDD), Know Your Customer (KYC), and Suspicious Activity Reporting (SAR) in a timely manner as required by law enforcement agencies. Addressing these weaknesses can enable banks to control ML to a considerable extent (Fraud.com, n.d.[16]).

As the digital economy expands, financial transactions are increasingly moving online, leading to a global banking system on the internet. The technological advancements in the banking sector have enhanced efficiency and convenience, but they have also been potentially misused to facilitate ML. The evolution of banking services, including internet banking, mobile banking, wire transfers and offshore banking, has further expanded the scope for ML activities (FATF, 2021 [17]). Information technology has transformed traditional banking into electronic banking and digital payment systems, while also introducing virtual currencies that present unique challenges in detecting ML. A virtual currency had been originally defined in 2012 by the European Central Bank, the governing monetary institution of the European Union, as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community."(European Central Bank, 2015 [18]). This complex definition captured both the abstraction and limitation of early virtual currencies, decentralized from government. The Financial Action Task Force (FATF) describes virtual currency as ‘virtual assets (crypto assets) refer to any digital representation of value that can be digitally traded, transferred or used for payment. It does not include digital representation of fiat currencies’ (FATF, n.d. [19]).

Blockchain technology and its associated cryptocurrencies, such as Bitcoin, are decentralized digital assets that are cryptographically secured against tampering (Suprayitno, Sari, Judijanto, Amalia, & Sukomardojo, 2024 [20]). Each unit can securely hold transactions over time within blockchain systems.The decentralization of blockchain and the anonymity of transactions pose significant challenges to financial security. The desire to liberate financial systems from government control has led to the rise of cryptocurrency (Hayek, 1976 [21]). Cryptocurrency transactions require minimal user information, such as location and company verification, without necessitating personal details. This increasing anonymity complicates efforts by law enforcement agencies to trace and intercept money laundered through cryptocurrency trading (Dyntu & Dykyi, 2018 [22]).

However, this unregulated environment can create conditions conducive to financial crimes (Litvishko, Beketova, Akimova, Azhmukhamedova, & Islyam, 2020 [23]). Authorities, including the Federal Bureau of Investigation (FBI), predict that the growing acceptance of Bitcoin among vendors and users will result in increased illicit financial activity and crime. Innovative tools must be integrated into the current financial and banking systems, necessitating updates to AML regulatory frameworks. It is essential to regulate virtual currencies as a new form of legal digital payment method. The issue of inconsistent cryptocurrency laws across various jurisdictions complicates the establishment of legal status and further hinders AML enforcement (Drozd, Lazur, & Serbin, 2017 [24]).

Several nations have begun implementing strict controls on cryptocurrency transfers to mitigate ML risks. However, Sri Lanka has yet to establish a legislative framework for cryptocurrencies within its AML system. The CBSL has cautioned against the risks associated with unregulated cryptocurrency in the financial system and emphasized the need for stringent controls or specific restrictions. Countries that are still developing cryptocurrency laws must acknowledge the risks associated with widespread use.

**4.3 Combating Money Laundering in Banking Systems**

Given the current scenario, it is of utmost importance to conduct a comprehensive evaluation of the existing legislation and supervisory frameworks in preventing banks and financial institutions from becoming targets of illicit activities. This concern is particularly significant in developing countries, where the banking institutions are relatively smaller as compared to those in developed economies. Such environments offer more opportunities for criminal elements to exploit. Moreover, the regulatory controls in place in developing countries to prevent criminal activities are relatively inadequate, less stringent and less effective than those in developed nations. This disparity makes them more vulnerable to manipulation by illicit actors. Therefore, it is crucial to assess the adequacy of regulatory mechanisms and strengthen them where necessary to mitigate the risks associated with criminal infiltration in the banking sector.

The situation described above has significant implications for the integrity of the banking system, which ultimately affects public trust in financial institutions (Claver, El Khoury, & Weeks-Brown, 2023 [25]). This loss of confidence can have a domino effect on the financial market, leading to the system's failure. Therefore, it is evident that the process of ML poses substantial risks to the overall economic well-being, as any destabilization of financial institutions can lead to a loss of reputation and confidence in the financial stability of the country. Financial experts assert that the reputation of banking institutions is closely tied to the stability of such institutions. This opinion reflects that depositors prefer to engage with institutions that are free of criminal clientele seeking to defraud the system. Widespread ML activities within a country's financial system can lead to sudden, unpredictable changes that can cause monetary instability, which is particularly common in developing nations with less effective regulatory frameworks.

The secretive nature of ML activities contributes to the creation of an informal economic sector, which intensifies the challenges of accurately gauging monetary and financial statistics. This highlights the pressing need for enhanced controls and measures to mitigate the adverse impacts of ML on economic stability. An important strategy in combating ML involves scrutinizing and monitoring the origins of suspicious funds as they enter the national financial system [Ibid n13]. However, a negative drawback of this approach is that customers may resort to engaging with alternative financial service providers who do not comply with AML regulations, often referred to as "informal financial channels."

The use of banks for illegal purposes can pose a significant threat to the Sri Lankan banking system (Ministry of Foreign Affairs, 2023 [26]). This can cause instability in financial institutions, leading to economic downturns which can provide opportunities for terrorist financing and capital flight. The financial system in Sri Lanka has been fragile in the past, as evidenced by the government's spending to rescue troubled financial institutions like Golden Key Credit Card Company and Sakvithi Investments (Gunaratne, 2008 [27]). This can have a detrimental impact on the economy, resulting in significant fiscal expenditures.

Further, the NRA for 2021/2022 has identified high-risk entities, including Hawala systems, which are informal and unregulated mechanisms for transferring value outside the formal banking sector, where physical currency does not change hands, allowing the transfer of funds to another party in a different country in local currency (Kagan, 2023 [28]). The system relies on trust, with the receipt for a transaction being something as simple as a playing card or a postcard torn in half. One half is kept by the customer, and the other is sent to the overseas Hawala banker. The launderer can then present their receipt in the destination country to access their funds, avoiding the need to transport illegal cash across borders physically. This eliminates the need for physical movement of money and conventional paper records, presenting significant challenges to regulate and monitor.

The NRA for 2021/2022 also identifies medium-risk entities across a variety of fields. Within the financial sector, securities trading entities including stockbrokers and primary dealers are vulnerable to manipulation, creating opportunities for ML. In addition, restricted dealers, despite their limited trading capacities, can still pose moderate risks due to potential regulatory loopholes. Legal professionals are also referred to as inadvertent participants who obscure the origins of illicit funds.

Even in sectors such as casinos and the gem and jewelry trade, there is a high potential to facilitate ML activities, which present significant opportunities for manipulating large sums of cash and concealing illicit funds. Casinos offer an environment where money can move freely, permitting persons to launder vast amounts of cash, through various gambling activities. Similarly, the gem and jewelry industry, which handles items of intrinsic value, such as precious stones and metals, is recognized as a high-value sector and is a targets for crime. This sector also significantly influences the potential conversion and movement of illicit funds. These results are applied to the country's AML/CFT policies for 2023-2028 to minimize recognized risks and enhance integrity in the financial system as a whole (Financial Action Task Force, 2024 [29]).

**4.4 Legal Regime on Money Laundering in Sri Lanka**

As aforesaid, Sri Lanka was blacklisted by the European Commission for ML risks due to major AML deficiencies. It has since been removed from the FATF's ‘Grey List' of high-risk countries after assessments by the review team, including the APG Secretariat, and has started implementing the FATF Action Plan (The Morning, 2019 [30]). Sri Lankan regulators have put in place strong AML laws to prevent banks and financial institutions from being affected by ML activities. However, there is still a potential risk of increasing ML activities targeting banks and other financial institutions. This risk is especially high due to the modernization of banking infrastructure and the financial sector as a whole.

**4.4.1 Prevention of Money Laundering Act (PMLA)**

ML is considered a criminal offence in Sri Lanka under the PMLA. The FATF has categorized ML as a predicate offense according to international standards. The PMLA has acknowledged this classification under section 3(1) and has criminalized the act of deriving or realizing property directly or indirectly from unlawful activities. The definition of the offence under the PMLA is broad and includes direct and indirect involvement in illegal activities, as well as actions such as receipt, possession, concealment, dispossession, transfer into or out of Sri Lanka or investment of any property realized from illegal activities. The mental element (mens  rea) or intent of the crime of ML is defined in the section as either having knowledge or having reason to believe. The efforts undertaken by legislators to incorporate a wide array of circumstances in terms of the commission of the offence of ML are commendable and appropriate in light of the significant implications that ML crimes have on the financial and economic stability of the country.

Section 35 of the PMLA defines "unlawful activity" by listing a range of acts and laws, making it easier to interpretation of this phrase. The term "unlawful activity" includes offences under other current laws as well. This means that ML is interpreted broadly in Sri Lanka, encompassing a broad array of offences as per the above interpretation and s. 3(b) of the PMLA. It is essential to note that the crime includes properties brought into and transferred out of Sri Lanka. Overall, this broad interpretation shows that the legislature has made significant efforts to cover all possible ways of committing ML under the law.

Also, under s. 3(2) of the PMLA, not only the act of ML is considered a crime, but also actions like conspiring, attempting, aiding and abetting. Additionally, bribery, terrorism, and other related offences are also considered ML offenses under the PMLA. This shows that the PMLA aims to be as comprehensive as possible in dealing with ML. The provisions of the Act have been designed to minimize potential loopholes that could be exploited by criminals to engage in ML activities. Overall, the PMLA takes a deliberate approach to ensure that it is as comprehensive as possible in dealing with ML.

1. 4 of the PMLA contains a rebuttable presumption which states that any movable or immovable property derived or realized from any illegal activity, directly or indirectly, is presumed to be beyond the known income or receipts of the person involved. In other words, if there is no clear and verifiable connection between the property and the individual's declared or known income, it is conclusively presumed that the property has been acquired from illegal activities. It is the responsibility of the accused to prove the contrary based on the balance of probabilities. This provision serves as a salutary feature of the PMLA as it is challenging to gather evidence to prove ML beyond reasonable doubt. Until the accused shows evidence to the contrary, as required by law, it is assumed that the property gained from unknown sources is the result of illegal activities. This legal provision is beneficial for those interpreting and implementing the law as it provides a legal framework to act when reasonable grounds are available to suspect the involvement of the accused in the offence of ML. Law enforcement officers can make use of this provision that necessitate swift action in situations where there is a risk of immediate disposal of illegal money. This provision proves practical when considering the difficulty in establishing guilt due to challenges in obtaining evidence. Additionally, the PMLA recognizes the transnational nature of ML and designates it as an extraditable offence, making it more effective across borders. Hence, it is justifiable to assert that the creators of this legislation have effectively discharged their responsibility by providing sufficient legal mechanisms for adjudication before the court. One of the main challenges faced by bankers is determining whether a property or sum of money is derived from a predicate offence. To assist this process, the law has established the above mentioned "rebuttable presumption”. As mentioned earlier, if the origin of the property cannot be linked to the known income of the accused under investigation, it is considered to have been obtained through unlawful means. This legal presumption is a tool to help identify and punish proceeds obtained from criminal avenues within the banking sector.

Given the detrimental impacts of ML and its adverse effects on the Sri Lankan economy and financial setup, the PMLA has reached out to the general public to create an obligation for people to disclose any knowledge or information about offences related to ML.  Section 5 of the PMLA imposes a legal obligation on the public to prevent such crimes. At the same time, S. 5(4) broadens the scope of this duty by explicitly stating that the duty to disclose overrides any other law that requires secrecy. Since the provision does not provide for exceptions, bankers are mandated to disclose any information pertaining to transactions of money from illegal activities to the FIU. Failing to disclose any information, whether intentionally or negligently, any knowledge or belief related to money or property stemming from illegal transactions also constitutes an offence of ML under S. 5(1) of the PMLA.

Furthermore, S. 6 criminalizes the sharing of information related to an investigation with a third party without permission. As a result, individuals who possess knowledge or suspicions regarding an ongoing or forthcoming investigation pertaining to ML are prohibited from disclosing such information or jeopardizing the investigation. Additionally, they are prohibited from divulging the identity of the person under investigation. Intentionally concealing or destroying any relevant documents or evidence related to the investigation can result in criminal charges. If found guilty, individuals may be fined up to one hundred thousand rupees or imprisonment for a maximum period of twelve months, or both. It is important to note that the 2011 amendment to the principal act of 2006 has increased the maximum fine and imprisonment duration from fifty thousand rupees and six months, respectively, to one hundred thousand rupees and twelve months.

It is important to note that tax evasion is not considered a crime under the PMLA. Nevertheless, substantial evidence suggests a symbiotic relationship between tax evasion and ML which cannot be ignored. ML, while aiding organized crime, also facilitates significant tax evasion, with specialists in this illicit practice honing their skills to conceal profits for affluent taxpayers evading their rightful tax obligations (Camacho, n.d. [31]). To strengthen AML efforts and fight against financial crimes, criminalizing tax evasion would not only eliminate existing loopholes but also serve as a potent deterrent against both tax evasion and ML activities. Such proactive measures are essential for maintaining the integrity of financial systems, promoting transparency and ensuring that every individual contributes their fair share to the collective welfare of society.  Therefore, it is necessary to address this lacuna in the current legal system by creating new laws specifically targeting tax evasion. This will strengthen AML measures and help to prevent financial crimes.

The current legal framework stipulates that law enforcement officers should be empowered to issue freezing orders to effectively enforce the legal provisions related to ML and mitigate its impact. Part 11 of the PMLA is dedicated to dealing with the freezing and forfeiture of assets that are associated with ML. Freezing Orders enable prompt intervention to prevent the use or transfer of assets linked to ML, effectively disrupting criminal operations and deterring further illicit transactions (Financial Action Task Force, 2010 [32]). The implementation of swift response empowers law enforcement officers to issue Freezing Orders swiftly, without the need for prior court approval, ensuring a quick reaction to suspicious activities. This enhances the efficacy of efforts to combat ML within the legal system.

A police officer not below the rank of an Assistant Superintendent of Police possesses the authority to impose a freezing order on any suspected property to facilitate an investigation. Such freezing order remains in force for seven days from issuance and can be extended to one year through an order from the High Court. Such police officer is required to obtain confirmation of the order from the High Court within seven days (S. 8 (1) PMLA). If the Court is satisfied with the reasons given, they can confirm and extend the Freezing Order (S. 8 (2) PMLA). This requirement for judicial confirmation within seven days ensure that there is a check on the police's power and that the orders are subject to legal scrutiny.The High Court is empowered to issue relevant orders to freeze and forfeit such assets as outlined in S. 8(1) and (2) of the PMLA. If an indictment is filed within one year, the freezing order remains valid till the conclusion of the trial. Subsequently, if the person is convicted, the freezing order remains in effect until the conclusion of any appeal process. These provisions are specified under sections 7 and 8 of PMLA and empower law enforcement agencies to take decisive action to prevent further dissemination of illegal funds and assets while investigations are ongoing.

Section 11 of the PMLA includes provisions that allow the High Court to appoint a Receiver to protect identified property. This is done to safeguard assets and protect legitimate claimants. A police officer of at least the rank of an Assistant Superintendent of Police can apply for this appointment. The Receiver is responsible for managing the frozen account, property or investment according to court directions. These provisions are important because they enable the state to intervene and prevent potential ML activities. This intervention is crucial because illegal activities can have a significant impact on the economic and financial stability of the nation and undermine the integrity of the existing legal framework. By allowing for the freezing and forfeiture of assets linked to ML, these measures contribute to safeguarding the integrity of the financial system and upholding the rule of law.

The PMLA was amended through the Act No. 40 of 2011 (PMLA - Amendment), representing another legislative measure aimed at addressing ML in Sri Lanka. The objective of this amendment was to strengthen the existing legal framework related to ML and to provide enhanced support to law enforcement authorities in combating such illegal activities. One notable amendment is the expansion of the scope of the Act to include anyone in Sri Lanka, regardless of residency (S.2, PMLA - Amendment). According to the provisions of the PMLA, if an individual is found guilty of committing the offense of ML and such commission is proven by law enforcement officers, the accused is liable to punishment and penalties.

The penalties for ML have also been broadened, with the amendment specifying the conditions under which a person can be convicted. The penalties now include fines ranging from no less than the value of the property involved to a maximum of thrice the value of the property, imprisonment for a period of 5-20 years, or both (S.3 PMLA - Amendment). The assets of the convicted party, including those acquired through ML, are liable to forfeiture (S.3 (1A) PMLA - Amendment). In cases where the offence has been committed by a corporate body or other entity, both the office bearers and any employee involved are held guilty for their actions (S. 18 (a) PMLA). These stringent measures are designed to deter and penalize persons and entities engaged in ML activities, thereby reinforcing the integrity of the legal system and safeguarding the financial well-being of the nation.

The PMLA - Amendment, also includes changes to various sections of the Act. Section 6 sees an increase in the maximum fine and imprisonment period. The maximum fine from fifty thousand rupees to one hundred thousand rupees and extends the maximum imprisonment from six months to twelve months. Section 7 lowers the rank of police officers authorized to perform certain duties. Section 11 undergoes a similar amendment, lowering the rank required for certain police actions. Procedural changes are also introduced by this amendment. Section 8 now requires "ex parte" applications within a seven-day window and limits the maximum period for any extension of a freezing order to three months at a time, with a total limit of two years. Section 9 clarifies that transactions can only be carried out with the sanction of the Court.

The PMLA - Amendment mandates the forfeiture of any property derived from unlawful activities upon conviction and introduces measures for cases where such property cannot be found (S.13 PMLA - Amendment). This includes requiring the payment of an equivalent value or imposing fines. The amendment also ensures that bona fide interests in property are considered and protected. Sections 14 and 15 are replaced with detailed provisions for restoring rights to bona fide claimants who can demonstrate legitimate ownership or control of property subject to a freezing order. Section 15 replacement allows the court to appoint a receiver to manage forfeited assets. New offenses are introduced by the amendment, including offenses for falsifying, concealing or destroying documents relevant to an investigation and for divulging information about ongoing investigations (S.20 PMLA - Amendment). These amendments collectively enhance the scope, enforceability, and penalties of the ML law, improve procedural clarity, and ensure that assets derived from unlawful activities are effectively managed and forfeited, while protecting the rights of legitimate owners.

**4.4.2 Financial Transaction Reporting Act (FTRA)**

Parallel to the PMLA, the Sri Lankan Parliament passed another notable legislative measure to combat ML. This legislation is known as the Financial Transaction Reporting Act No.6 of 2006 (FTRA). It established the Financial Intelligence Unit of Sri Lanka (FIU) as per the requirements under recommendation 29 of FTAF 40 recommendations. The significant outcome of this enactment was the establishment of the FIU that serves as the apex authority overseeing AML laws and regulations within Sri Lanka. The FIU is vested with statutory powers to scrutinize suspicious financial transactions and to conduct thorough investigations into instances of ML and TF. The FIU functions as a centralized repository for receiving relevant information, monitoring financial activities and executing necessary actions as stipulated by the provisions of the FTRA. Moreover, the FIU is mandated to assist in the collection of data relating to sources, prevention, detection, investigation and prosecution measures associated with ML and related offenses. The FIU plays a crucial role in protecting Sri Lanka's financial system from illegal activities, as outlined in s. 15(1) of the FTRA. Sri Lanka's FIU has been accepted into the Egmont Group, a global association of Financial Intelligence Units founded in 1995, demonstrating the country's commitment to combating financial crimes through international cooperation.

The FTRA imposes significant legal obligations on financial institutions and designated non-financial institutions. These obligations include the enforcement of Know Your Customer (KYC) principles, preventing the unlawful use of banking products and services for ML purposes and assisting in investigations by monitoring suspicious financial transactions.

According to S. 1 of the FTRA, it is mandatory to properly identify the account holder before opening an account. This means that customers must fulfill the necessary KYC requirements before opening an account. Additionally, the Financial Institutions (Customer Due Diligence) Rule No 1 of 2016 provides specific instructions for the identification procedures for different types of customers. If an account holder cannot be identified or has provided a fake name, financial institutions are prohibited from maintaining or operating that account, as stated in S. 2(1) of the FTRA. If the identity of the account holder cannot be ascertained, institutions must not execute any transactions and should report it to the FIU promptly. Moreover, S. 2(2) of the FTRA requires banks to take all appropriate measures to diligently identify their customers.

FIUs are crucial in the fight against ML. They receive, analyze and disseminate information both domestically and internationally. Although there may be variations between countries, all FIUs have these core functions and rely on effective information sharing mechanisms. Financial institutions are required to report suspicious activities to the FIU. Centralizing this function ensures efficiency and enhances prevention efforts. In Sri Lanka, the Administrative Model is used for its FIU. It is established within the CBSL and reports directly to the Governor and Monetary Board, as outlined in Gazette Order No.1437/24 of March 23, 2006 (Financial Intelligence Unit of Sri Lanka, n.d.and International Monetary Fund, n.d. [33]). The FIU Director reports to the CBSL Governor via an Assistant Governor. The FIU handles reported cases independently, in collaboration with law enforcement agencies.

***4.4.2.1 Monitoring Mechanisms***

FTRA s. 5 mandated that financial institutions to carry out thorough customer due diligence and maintain records accordingly. This is important as it ensures ongoing vigilance in detecting any illegal activities related to ML, particularly considering that a customer's status may change over time. This could result in situations where the initial KYC process conducted during the account opening stage may not be sufficient to detect any instances of ML. To verify the identity of account holders, banks may request documents such as the National Identity Card and utility bills to verify the address. Additionally, banks may send a welcome letter to the provided address to obtain confirmation of the address. Furthermore, this Act stipulates that financial institutions must implement effective monitoring mechanisms for all transactions and promptly report any suspicious activities.

Suspicious activities may include unusual transaction patterns, multiple accounts opened across different branches with identical addresses, large deposits followed by immediate electronic withdrawals and accounts with low balances but substantial sums being transferred through them (Financial Intelligence Unit, CBSL, 2018 [34]). If any suspicious activity is detected, financial institutions are required to notify the FIU within two days. It is important to note that once a report has been submitted, banks are prohibited from disclosing any information to the customer in order to ensure the integrity of the investigation process.

***4.4.2.2.Reporting Requirements***

Financial institutions are obligated under sections 5, 6 and 7 of the FTRA to report electronic fund transfers and suspicious transactions exceeding Rs. 1,000,000/-, or any other threshold amount specified by the Minister of Finance. In July 2023, the Merchant Bank of Sri Lanka and Finance PLC faced a fine of Rs. 300,000 due to its failure to report pawning auction transactions that exceeded Rs. 1 million, as mandated by Section 19 (1) and section 19 (2)  of the FTRA. Similarly, Vallibel Finance PLC has been fined Rs. 200,000 for failing to report transactions that exceeded Rs. 1 million. Similarly, LB Finance PLC incurred a penalty of Rs. 700,000 for not reporting pawning auction transactions that surpassed the Rs. 1 million threshold. In addition, People's Leasing & Finance PLC has been fined Rs. 500,000 for not reporting an electronic fund transfer associated with the opening of a fixed deposit that exceeded Rs. 1 million (Sunday Times, 2023 [35]). These incidents highlights the importance of compliance with the regulatory framework established by the FTRA which requires banks to report large transactions to the FIU. The FIU collected penalties as indicated above, amounting to Rs. 1.7 million in total from April 1, 2023 to September 16, 2023 to enforce compliance on financial institutions [35].

‘From May to October 2024, the FIU imposed administrative penalties on various Reporting Institutions for non-compliance with the FTRA. The total penalties collected amounted to Rs. 2,750,000, which were credited to the Consolidated Fund. MCB Bank Ltd was fined Rs. 1,000,000 on July 26, 2024, for failing to report Electronic Fund Transfer (EFT) transactions exceeding Rs. 1,000,000 as mandated by the FTRA regulations. Similarly, the Bank of China Ltd faced a penalty of Rs. 1,000,000 on September 10, 2024, for the same reporting failure regarding EFT transactions. Vogue Jewellers (Pvt) Ltd was imposed an administrative penalty of LKR 750,000. The penalty was due to the company's non-compliance with the FTRA and related regulations. Specifically, the company failed to obtain identification documents from customers engaging in cash transactions of USD 15,000 or more, as mandated by the FTRA and the Customer Due Diligence (CDD) Rules. Additionally, it did not maintain or retain the required records of identification documents of customers as required by the Section 4(1)(b) of the FTRA and Rule 38(1) of the CDD Rules’(Central Bank of Sri Lanka, 2024 [36]).

If an institution suspects that a transaction may be linked to ML or TF, they are required to report it immediately (S. 7 FTRA). For the purposes of the FTRA, an "institution" is defined as a person or body of persons who are professionally engaged in conducting financial business or designated non-finance business (S.33 - Interpretation Clause - FTRA). Furthermore, section 5(1) of the FTRA requires individuals who have knowledge or reasonable grounds to believe that property has been acquired through unlawful activities to file a suspicious transactions. It is mandated that financial institutions maintain records of their business activities for at least six years from the date of the transaction (S. 4 (1) (a) & (b), FTRA). If there is an ongoing legal proceeding, the obligation to retain records extends beyond the standard six-year time frame.

Financial institutions are required to appoint a compliance officer to ensure compliance with the provisions of the FTRA. The FTRA regulations, dated June 26, 2006, mandate that banks must have the capability to accurately identify and verify all the KYC details of their customers, in order to substantiate their claimed identities. Providing false information is considered an offence under section 28 of the FTRA, and carries severe consequences. Section 28(6) further specifies that authorizing, operating or opening of accounts under fictitious or false names of an institution constitutes a punishable offence. The offences under the FTRA are categorized as cognizable and non-bailable, highlighting the serious nature of violations. Any falsification of documents is also explicitly prohibited and constitutes an offence under the FTRA. Part IV of the FTRA deals with extradition and mutual assistance concerning the offence of ML, which helps our country align with the international community. The FTRA also defines and delineates unlawful activities, a crucial aspect of its provisions.

**4.4.3 Legislative and Regulatory Reforms in AML/CFT**

In addition to aforementioned legislative frameworks, Sri Lanka has undertaken further significant regulatory reforms aimed at strengthening its AML/CFT framework. These initiatives represent a proactive approach to enhance compliance and mitigate risks associated with financial crimes. There are other key statutes that, although not exclusively focused on AML/CFT, play a notable role in shaping the overall compliance landscape. The Banking (Special Provisions) Act, No. 17 of 2023, requires all banks implement essential AML/CFT measures like customer due diligence (CDD), transaction monitoring and reporting of suspicious activities to the FIU, thereby reinforcing adherence to AML standards across the sector. The Regulation of Insurance Industry Act No. 43 of 2000 obligates insurance companies to adopt AML/CFT controls like CDD and transaction oversight. Additionally, the Insurers (Customer Due Diligence) Rules, No. 1 of 2019, were enacted to impose stringent customer due diligence (CDD) requirements on insurance companies, thereby fortifying the sector's compliance capabilities (Financial Intelligence Unit of Sri Lanka, n.d. [37]).

The Central Bank of Sri Lanka Act, No. 16 of 2023, to further strengthen the Central Bank's supervisory capacity, indirectly promotes AML initiatives and notes that astute coordinated efforts with the FIU is essential for success in AML law enforcement. This Act is pivotal for maintaining financial stability and ensuring compliance with AML/CFT standards across financial institutions. Furthermore, the Payment and Settlement Systems Act No. 28 of 2005 incorporates provisions that require payment service providers to adhere to transaction monitoring and reporting obligations, thereby integrating AML/CFT considerations into payment systems.

To facilitate compliance with these statutes, the FIU has issued various regulations and guidelines covering Customer Due Diligence (CDD), record-keeping (Financial Intelligence Unit, 2023 [38]), and reporting suspicious transactions (STR) (Financial Intelligence Unit, 2019 [39]). CDD regulations require that financial institutions check the identities of their customers and continuously monitor their transactions to prevent criminal activities. The issuance of Direction No. 01/2020, which establishes protocols for engaging compliance officials during weekends and holidays, ensures timely resolution of compliance issues [34].

Further amendments to the Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016, published in 2018, have updated CDD requirements for financial institutions, addressing previously identified vulnerabilities. The introduction of the Designated Non-Finance Business (Customer Due Diligence) Rules, No. 1 of 2018, has expanded the AML/CFT measures to encompass non-financial businesses, thereby broadening the regulatory scope. The foundational Financial Institutions (Customer Due Diligence) Rules, No. 1 of 2016, continue to provide a comprehensive framework for financial institutions to enhance their compliance efforts.

Moreover, the Guidelines on AML/CFT Compliance Obligations for Attorneys-at-Law and Notaries, No. 02 of 2023, issued under Section 15 (1) (j) of the FTRA, established a comprehensive framework aimed at assisting legal professionals in fulfilling their obligations related to AML/CFT (Financial Intelligence Unit, 2023 [40]).

These regulatory changes in Sri Lanka signify the country's dedication to enhancing its AML/CFT framework. However,despite these efforts, major gaps and inadequacies within the regulatory framework often make the effective enforcement of AML rules difficult. Many institutions cannot meet these requirements effectively due to incomplete verification systems and reliance on outdated technology.

**4.4.4 Enforcement Mechanism for AML in Sri Lanka**

In Sri Lanka, the implementation of AML/CFT measures is mainly entrusted to the FIU in collaboration with various law enforcement agencies, such as the police and customs. However, several challenges and strengths have come to light when analyzing the enforcement landscape in Sri Lanka. At the head of them is an issue of resource constraints and institutional capacity that seriously affect enforcement effectiveness and compliance. Due to this resource constraints, agencies are restricted in their ability to employ effective AML measures. Another critical issue is delayed reporting and assessment. Timely reporting of suspicious transactions coupled with regular risk assessments are essential for effective AML initiatives. Moreover, the problem of effective AML/CFT measures enforcement is hampered by procedural inefficiencies and inadequate inter-agency cooperation among various law enforcement agencies. Strengthening co-ordination between each agency involved in these efforts is essential to resolve this interagency gap. Further, endless judicial procedures also delay prosecution and enforcement efforts (International Monetary Fund & World Bank, 2004 [41]). Therefore, policy reforms should be introduced to close legal loopholes and improve overall compliance.

**4.4.5 Sri Lanka’s Engagement in Global and Regional Organizations**

Sri Lanka undergoes a national reform to bring its AML framework into line with international standards. As part of its obligations to the International Monetary Fund (IMF), Sri Lanka must enhance its AML/CFT framework to align with international standards, which is also integral to broader economic reforms. Former president Ranil Wickremesinghe has underlined the importance of an impending exposure to attract foreign investment and promote Sri Lanka's business climate. The government strives to resolve existing bureaucratic difficulties and simplify legal procedures necessary for a more enabling environment to develop (Ada Derana, 2024 [42]).

International standards on ML are established by prominent global organizations, including the FATF, the APG and the Egmont Group. The FATF's 40 Recommendations delineate fundamental components necessary for the establishment of effective AML/CFT frameworks, emphasizing the importance of risk-based methodologies, customer due diligence and effective enforcement (Financial Action Task Force [FATF], n.d. [43]). The APG functions as a regional monitoring entity within the framework established by the FATF. Its primary role involves aiding member jurisdictions in the effective implementation of AML/CFT efforts through international cooperation and the exchange of financial intelligence (FATF, n.d. [44]).

Sri Lanka was scheduled for its third mutual evaluation by the APG in March 2025, following a history of challenges in previous assessments. As aforementioned Sri Lanka experienced dual grey listing by the FATF and has been blacklisted by the European Union due to its failure to comply with established regulatory standards. These grey and black listing has adversely affected Sri Lanka’s international standing and economic relations, highlighting deficiencies in its AML/CFT framework (FT.lk, 2025 [45]). These actions have resulted in considerable challenges that have negatively impacted the country's international reputation and economic relations. Specifically, inclusion on the FATF grey list can precipitate substantial financial and reputational repercussions, including restricted access to global financial markets, diminished foreign direct investment, increased compliance costs and the potential for credit rating downgrades (de Koker, Howell & Morris, 2023 [46]). Sri Lanka is strategically aligning its regulatory framework with the standards established by the APG and the Egmont Group. This alignment is intended to mitigate potential economic consequences associated with being placed on the FATF and strengthen Sri Lanka’s ability to combat financial crime.

In preparation for this impending review, Sri Lanka’s FIU has actively engaged with 24 stakeholders and sought insights from a high-level APG delegation, which included key figures such as Mr. Julien Brazeau, Dr. Gordon Hook and Mr. David Shannon [45]. Their visit highlighted several critical areas for improvement, including the effectiveness of the AML/CFT system in addressing the country's risks, enhanced monitoring of progress and operational outcomes, timely legislative reforms related to AML/CFT, adequate resource allocation for implementation, improved inter-agency coordination, capacity building for prosecutors, law enforcement and the judiciary, increased private sector engagement in supporting AML/CFT efforts and stronger international cooperation to combat financial crime (Asia/Pacific Group on Money Laundering [APG], 2023 [47]).

Sri Lanka's third evaluation of its AML/CFT framework has been postponed by one year and is now set to commence in March 2026, as indicated by the CBSL. The delay is attributed to the two national elections that occurred last year (ECONOMYNEXT, 2025 [48]). Analysts warn that if Sri Lanka does not implement effective AML/CFT measures recommended by the global bodies, it risks falling into the grey list for a third time, which could hinder the country's economic recovery following a sovereign debt default [48].

The third Mutual Evaluation, coordinated by the APG, will assess Sri Lanka's efforts against ML and TF. The CBSL emphasized the need for compliance with the 40 recommendations from the FATF and the effectiveness of its AML/CFT framework based on the FATF's 11 immediate outcomes [48]. To promote its AML/CFT examinations, the CBSL plans to enhance risk-based assessments of banks in accordance with the FTRA and FATF recommendations. The high-level AML/CFT Task Force, reconstituted in December 2024, will remain active until the successful completion of Mutual Evaluation in July 2027. Sri Lanka is required to enact several measures, including new laws to meet AML/CFT standards before the next evaluation [48].

This question is answered by the updated national risk assessment (NRA) of the FIU, set to be conducted by the FIU in the second quarter of this year, including evaluations on tax crimes and proliferation of financing risks. The FIU aims to enhance cooperation with non-financial institutions and their regulatory authorities by forming several working groups. Additionally, the FIU has been advocating for compliance with AML/CFT obligations and is working on FATF compliance measures as part of a request from the International Monetary Fund (IMF), which has linked compliance to Sri Lanka's $3 billion package [48]. The FIU is also finalizing amendments to key AML/CFT legislation to strengthen the legal framework in line with international standards, as the country has faced serious risks from ML and TF over the past 14 years.

Further, Sri Lanka has shown its commitment towards fighting illicit activities by signing and ratifying major international treaties such as the Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, the United Nations Convention Against Transnational Organized Crime, the United Nations Convention Against Corruption, and the Convention to Combat Terrorist Financing, as recommended by FATF (United Nations Office on Drugs and Crime [UNODC], 2023 [49]).

**5. THE ANALYSIS**

It is evident that Sri Lanka has taken significant steps in creating a regulatory framework to combat ML. The AML laws and banking practices are crucial in improving the effectiveness of AML efforts. The legal framework is designed to prevent, detect and take legal action against ML activities and banking practices are essential for implementing measures to ensure compliance with AML regulations.

Both the PMLA and the FTRA contain penalties and sanctions for ML activities and non-compliance with AML protocols. Despite these efforts, there are still notable gaps and deficiencies in Sri Lanka's AML mechanisms. One such gap is the lack of regulations monitoring the financial activities of charitable and non-profit organizations. This lack of oversight makes these entities vulnerable to being exploited for unlawful financial activities without adequate scrutiny.

The financial sector has rapidly evolved globally, creating new opportunities for ML in areas such as crypto-currency or digital currencies. However, the anonymity involved in such transactions has led to an accelerated rate of ML, making it difficult for traditional AML frameworks to combat such activities effectively (Davies, n.d. [50]). Similarly, the current AML regime in Sri Lanka is not adequate in addressing ML that results from technological advancements. As technology evolves, money launderers also develop new methods and tools, highlighting the need for a more adaptable and rigorous AML framework (Barr, Gifford, & Klein, 2018 [51]). There is also a need for policies that enhance international cooperation in combating ML (McDowell & Novis, 2001 [52]). However, such policies should align with existing AML frameworks to ensure consistency and effectiveness.

There have been concerns raised by entities such as Transparency International Sri Lanka regarding the Sri Lankan government's policy on foreign currency deposits, which allows deposits to be made without any questions being asked (Transparency International Sri Lanka, 2020 [53]). This policy undermines important processes such as KYC and AML, which increases the risk of ML activities. While Sri Lanka has made some progress in implementing AML measures, it is important to address any deficiencies, adapt to technological advancements, and strengthen international cooperation to make the AML regime more effective.

However, despite developing a legal framework to combat ML and TF in alignment with FATF's core principles and global development, criticisms still exist regarding the adequacy and effectiveness of Sri Lanka's laws in dealing with the challenges posed by ML. Although the current laws have mandatory obligations for financial institutions, including client identity verification, transaction record-keeping, internal reporting of suspicions and the appointment of designated officers for ML reporting, some observers consider them insufficient and less stringent. The financial sector contends that complying with these obligations requires significant expenditures on administration, training, supervision and legal compliance. However, proponents contend that computer systems can facilitate efficient compliance if they are properly programmed.

The KYC requirement is recognized globally for its effectiveness in deterring money launderers (Culp, 2015 [54]). However, it may impact the number of customers and the volume of work for financial institutions. Institutions that already have well-developed procedures in these areas will find the costs of compliance relatively less. The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is another system that poses a risk to authorities. SWIFT handles the registration of certain Business Identifier Codes approved by the International Organization for Standardization (ISO). However, it is impossible to differentiate between genuine customers and potential money launderers, even though banks require authentic documents to effect SWIFT. This raises concerns about the possibility of laundering funds through legitimate SWIFT transactions. Furthermore, regulatory authorities face obstacles posed by underground banking networks, commonly referred to as "parallel" banking such as Hawala, which operate outside the formal financial system and evade regulatory oversight. These systems follow traditional banking practices and use highly efficient methods to transfer funds globally.

In addition to the laws mentioned earlier, AML policies include all regulations and laws that require financial institutions to monitor their clients actively. This is done to prevent instances of ML and corruption. Developed nations have established specialized investigation units that are equipped with the necessary expertise to conduct thorough examinations of complex financial transactions involving international fund transfers and digital platforms. However, Sri Lanka lacks such specialized recruitment mechanisms. Instead, they rely on ordinary police officers from units like the Criminal Investigation Department (CID), Police Narcotic Bureau and Terrorist Investigation Division (TID) to handle these complex investigations. Therefore, it is of paramount importance to provide these officers with comprehensive training on relevant legal provisions, current trends in ML activities, advanced technologies and financial report analytical skills. With such extensive knowledge and experience, their ability to prosecute ML cases may be protected, without leaving room for defense counsels to exploit legal loopholes and procedural defects in investigation procedures.

In summary, while Sri Lanka has made efforts to improve its AML/CFT framework, there are still challenges to overcome, such as the effectiveness of existing laws and the emergence of new methods used by money launderers. Sri Lanka is still struggling to address deficiencies in its AML framework. The current criminalization measures against ML and TF are deemed insufficient. These shortcomings, include an inadequate legal foundation and insufficient procedures for asset freezing etc, making it challenging to effectively combat ML activities in the country. Addressing these issues will require ongoing evaluation and adaptation of regulatory measures to effectively combat ML and FT activities.

**5.1 Recommendations for Enhancing Sri Lanka's Anti-Money Laundering Framework**

Preventing ML is crucial for maintaining the stability and integrity of Sri Lanka's financial system as well as ensuring the overall economic well-being of the country. However, Sri Lanka faces significant challenges due to limited resources, weak implementation processes and widespread corruption. To effectively counteract ML, there are recommendations to address these issues.

**5.1.1 Strengthen AML Laws and Regulations:** It is important to strengthen AML laws and regulations. An effective legal framework is necessary to identify, investigate and prosecute ML activities. Sri Lanka can benefit from from revising its existing laws to address gaps and ambiguities and developing clear and comprehensive legislation helps to ensure that financial institutions and other relevant entities understand their obligations and can effectively implement preventive measures.

**5.1.2 Strengthening Regulatory Bodies:** Sri Lanka should enhance regulatory agencies like FIU, CID, TID, responsible for overseeing financial institutions and enforcing AML regulations. These agencies should conduct regular audits, inspections and examinations to ensure compliance and detect suspicious activities.

**5.1.3 Strengthening AML Enforcement:** To combat ML effectively, Sri Lanka must prioritize the **enhancement of its AML enforcement mechanisms**. While the legal framework exists, the primary challenge lies in **poor enforcement** and **practical difficulties in implementation**. Strengthening enforcement will not only improve compliance but also create a **naming and shaming deterrent**, discouraging industries and professionals from facilitating illicit financial activities.

**5.1.4 Independence of FIU:** To facilitate impartial and effective implementation of AML laws, it is crucial to ensure the independence of the FIU and other legal authorities from political interference. Political interference in investigation procedures not only undermines the integrity of the process but also emboldens criminals in their unlawful activities. The Bribery Commission can play a vital role in holding corrupt public officials accountable for aiding and abetting in such offenses.

**5.1.5 Establish specialized investigation units:** Establish specialized investigation units within law enforcement agencies that possess expertise in complex financial transactions and utilize advanced technologies such as artificial intelligence (AI) and facial recognition software for effective detection and prosecution of ML offences is essential.

**5.1.6 Stricter Regulatory Compliance:** To strengthen regulatory oversight of financial institutions, mandating stringent due diligence procedures accompanied by comprehensive KYC rules and appointment of compliance officers to ensure strict adherence to AML regulations is proposed (Huber, Memminger, Soppitt, & Hayday, n.d. [55]). It is important to strictly enforce the appointment of compliance officers by both financial and designated non-financial entities to prevent regulatory breaches.

**5.1.7 Inter-agency Coordination:** To ensure successful prosecutions and mitigate gaps in investigation procedures, enhance coordination and collaboration should be strengthen among various law enforcement agencies, including Sri Lanka Customs, Police Narcotic Bureau, CID, TID, FIU and the Attorney General's Department to ensure successful prosecutions against money launderers and for effective and efficient operation. The limited number of successful prosecutions for ML demonstrates weaknesses in investigation procedures and the lack of coordination among enforcement agencies.

**5.1.8 Capacity Building and Training:** Comprehensive training programs should be provided to law enforcement personnel such as police, CID, and FIU officers. These programs should focus on the latest trends in ML activities, digital forensic techniques and financial report analysis skills to enhance their investigation capabilities. Capacity building efforts should not just be limited to law enforcement authorities but should also include financial institutions who act as the gatekeepers of ML offences. If bank and financial institution employees lack knowledge regarding applicable AML laws and reporting requirements, it can provide criminals with opportunities to bypass legal barriers. These institutions play a crucial role in the primary point of contact with criminals in the ML process, which makes it imperative for them to enforce strict due diligence procedures and educate staff to efficiently identify red flags of ML. The KYC rule should not be treated as a compliance exercise only. Banks should be responsible for identifying suspicious transactions and reporting them promptly and there should be no tolerance for bank personnel tipping off customers. It is vital to take decisive action against corrupt employees and public officials to enhance the effectiveness of AML framework in Sri Lanka.

**5.1.9 Imposition of Monetary Penalties:** To discourage regulatory breaches and promote a culture of compliance, stricter monetary penalties must be imposed on financial institutions and designated non-financial businesses for non-compliance with the provisions of the FTRA and PMLA. This could involve increasing fines and custodial sentences for entities and individuals who fail to comply with AML/CFT requirements. While banks and finance companies have recently faced fines imposed by the FIU, there is a lack of records for penalties against non-financial individuals and entities. The enforcement actions will be increased to deter such breaches.

**5.1.10 Public Awareness and Education:** To enhance intelligence gathering capabilities, public awareness campaigns should be launched to educate the general populace about the detrimental impacts of ML. Educating the public about the negative impacts of ML and unlawful activities is crucial to promote cooperation and provide intelligence for successful examinations by the FIU and other authorities. This also will encourage them to report suspicious activities to authorities and promote cooperation in combating ML.

**5.1.11 Professional Collaboration:** Non-financial industries and professions must enhance their compliance arrangements to ensure the effectiveness of Sri Lanka's AML legal framework. Collaboration between professional organizations such as the Chartered Institute of Sri Lanka, Bar Association and Accounting Monitoring Board with the FIU should be facilitated to enhance compliance arrangements and educate their members on AML best practices and economic and social repercussions of ML.

**5.1.12 Implementing Cross-Border Currency Regulations:**

To combat illegal remittance businesses like Hawala and to detect cross-border currency smuggling, regulations empowering the CBSL to regulate cross-border currency smuggling effectively should be issued under Section 24 of the FTRA. Currently, there are no such regulations in place, indicating the need to introduce currency declaration requirements. Countries like Singapore, India and Malaysia, among others in the region, have already implemented specific declaration requirements for cross-border currency movements. In Sri Lanka, the existing declaration requirement falls under the Customs Ordinance, which may not be effective in identifying ML activities. Therefore, it is necessary to strengthen and formalize declaration requirements under the FTRA to improve the country's ability to detect and combat ML efforts effectively. Additionally, increased supervision of money changers should be implemented.

**5.1.13 Balancing Financial Inclusion and AML Measures:** To balance financial inclusion and AML measures, it's important to promote financial inclusion policies while implementing strong AML measures. This can be achieved through digital onboarding initiatives while mitigating the risk of financial service exploitation by money launderers.

**5.1.14 Stengthening Data Protection and Biometric Identity Measures:** Further strengthening data protection legislation and biometric identity cards implementation serve as a deterrent against the misuse of identification documents by criminals. This aligns with similar measures implemented in advanced jurisdictions such as Singapore to combat ML amidst rapid technological and financial industry advancements.

**5.1.15 Strengthening AML Measures in Digital Finance:** The Foreign Exchange Act No. 12 of 2017 lacks provisions that enable the CBSL to take legal actions against illegal remittance businesses. This regulatory gap hinders the implementation of AML laws in the country. However, it is essential that AML laws do not obstruct Sri Lanka's financial inclusion policy. The COVID-19 pandemic highlighted the significance of digital onboarding procedures for customers to conduct banking transactions seamlessly during such crisis situations. Apps like "FRIMI" gained popularity in Sri Lanka during the pandemic, emphasizing the need to maintain a balance between digital onboarding and preventing the abuse of financial services by money launderers.

By implementing these recommendations, Sri Lanka can strengthen its legal and administrative framework, enhance controls and effectively combat ML activities. This will help safeguard its financial integrity and stability. In Sri Lanka, it is crucial to protect the financial system's integrity, which requires building and promoting a culture of compliance. Such a culture should ensure adherence to regulatory mandates and serve as a vital tool for law enforcement agencies in their efforts to prosecute and punish individuals exploiting the financial system to launder illegal funds. By prioritizing the development of a compliance-focused mindset, Sri Lanka can effectively strengthen its financial defenses, reduce the risks associated with ML activities and increase the country's ability to withstand financial crimes.

**6. CONCLUSION**

The discourse on mitigating ML in Sri Lanka highlights the seriousness of this global criminal activity and its impact on the stability and integrity of the banking and financial sectors. Sri Lanka has demonstrated a thorough understanding of the multifaceted threats posed by ML. The examination of Sri Lanka's efforts to mitigate ML reveals a complex landscape that includes significant legislative progress, but also persistent enforcement challenges. Although the country has established a stringent legal framework aligned with international standards such as the FATF recommendations, the effective implementation of AML laws remains inadequate. The susceptibility of the banking system to exploitation by money launderers persists, exacerbated by ongoing technological advancements and the expanding array of banking services. Despite efforts to strengthen AML regulations and enhance enforcement measures, Sri Lanka still faces challenges such as insufficient monitoring systems, weak enforcement capacity and delays in legal proceedings.

In order to overcome these shortcomings, it is crucial for Sri Lanka to prioritize the continuous evaluation and improvement of its AML systems, ensuring they are capable of adapting to evolving threats. Collaboration with other jurisdictions is essential to prevent money launderers from exploiting regulatory loopholes and moving their operations to more favorable environments. In addition, the country should focus on using advanced technological tools to enhance its ability to detect, track and prevent ML activities. To promote a culture of responsibility and vigilance against financial crimes, public awareness campaigns and educational initiatives should also be intensified.

As Sri Lanka aspires to emerge as a global financial center, particularly with initiatives like the port city development, heightened vigilance against ML is imperative. The emergence of casinos and gambling, supported by politically exposed persons (PEPs), highlights the need for stringent AML enforcement measures, particularly in the digital space. Furthermore, the transnational nature of ML necessitates collaborative efforts with other jurisdictions to prevent launderers from exploiting regulatory disparities and relocating their operations. The adoption of innovative technological tools for detection and prevention is pivotal in augmenting AML efforts, although it is acknowledged that complete eradication of ML remains elusive. This requires a multi-faceted strategy, encompassing legislative reforms, stronger enforcement mechanisms, enhanced international cooperation, public awareness campaigns and technological advancements. Mitigating ML in Sri Lanka requires a proactive and concerted effort from all stakeholders across different sectors. By addressing the identified challenges and embracing a proactive stance towards combating financial crimes, Sri Lanka can enhance its resilience against the pervasive threat of ML. This, in turn, will help safeguard its economic prosperity and standing in the global financial community. By doing so, Sri Lanka can protect its economy and ensure the integrity and stability of its financial system in the face of evolving threats posed by ML.

**DISCLAIMER (ARTIFICIAL INTELLIGENCE)**

The author declare that she wrote this research paper independendently without any assistance from AI. However, the author utilized ChatGPT and the QuillBot AI Paraphrasing Tool during the editing process to enhance the overall language quality in a few sections.

Details of the AI usage are given below:

ChatGPT

QuillBot AI Paraphrasing Tool

**Competing interests**

Author has declared that no competing interests exist.

**Reference:**

1. Patabendige, C. (2023). Analysis of money laundering in Sri Lanka: A national security saboteur. International Journal of Security Studies & Practice, 3(1), Article 7. <http://ijssp.ung.edu>
2. EconomyNext. (2023, October 4). Sri Lanka CB comes up with IMF-urged anti-money laundering moves; asks lawyers to comply. <https://economynext.com/sri-lanka-cb-comes-up-with-imf-urged-anti-money-laundering-moves-asks-lawyers-to-comply-133669/>
3. Central Bank of Sri Lanka. (n.d.). The Financial Action Task Force delisted Sri Lanka from the Grey List. <https://www.cbsl.gov.lk/en/node/6701>
4. Gunawardena, N., & Maharoof, S. (2019). Understanding the risks of money laundering in Sri Lanka. <https://www.ft.lk/Opinion-and-Issues/Understanding-the-risks-of-money-laundering-in-Sri-Lanka/14-674510>
5. Financial Action Task Force (FATF). (2020). Follow-up report to Sri Lanka's assessment of anti-money laundering and counter-terrorist financing measures. <https://www.fatf-gafi.org/en/publications/Mutualevaluations/Fur-sri-lanka-2020.html>
6. Ministry of Justice. (2023). National policy on anti-money laundering and countering the financing of terrorism (AML/CFT) of Sri Lanka 2023–2028. <https://www.moj.gov.lk/images/pdf/2023/National_AML_CFT_Policy_2023-2028.pdf>
7. Ferwerda, J., Deleanu, I. S., & Unger, B. (2019). Strategies to avoid blacklisting: The case of statistics on money laundering. PLoS ONE, 14(6), e0218532. <https://doi.org/10.1371/journal.pone.02185328>
8. Bank Negara Malaysia. (n.d.). Money laundering & terrorism financing. [https://amlcft.bnm.gov.my/what-is-money laundering#:~:text=Money%20laundering%20is%20a%20process,to%20disguise%20its%20criminal%20origin.&text=Proceeds%20of%20an%20unlawful%20activity%20or%20instrumentalities%20of%20an%20offence.](https://amlcft.bnm.gov.my/what-is-money-laundering#:~:text=Money laundering is a process,to disguise its criminal origin.&text=Proceeds of an unlawful activity or instrumentalities of an offence.)
9. Ceylon Today. (2023, July 10). Role of non-banking financial institutions in facilitating money laundering and terrorist financing. <https://ceylontoday.lk/2023/07/10/role-of-non-banking-financial-institutions-in-facilitating-money-laundering-and-terrorist-financing/>
10. Levi, M., & Reuter, P. (1997). Money laundering. Crime and Justice, 34(1), 289–375. <https://doi.org/10.1086/501508>
11. Heart, M. (2019, November). Analysis of the proposed proceeds of crime legislative and policy framework in Sri Lanka. <https://www.tisrilanka.org/wp-content/uploads/2019/12/POCA-Report_Eng.pdf>
12. Fundanga, C. M. (2003, January 23). The role of the banking sector in combating money laundering. Paper presented at a seminar organized by the C and N Centre for Advanced International Studies, Lusaka, Zambia. <https://www.bis.org/review/r030212f.pdf>; Thommandru, A., & Chakka, B. (n.d.). Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks. Sustainable Futures, Elsevier. <https://www.sciencedirect.com/journal/sustainable-futures>
13. International Monetary Fund (IMF). (2023). 2023 review of the Fund’s anti-money laundering and combating the financing of terrorism strategy. <https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015>
14. Brada, J. C., Drabek, Z., & Perez, M. F. (n.d.). Money flows as motives for FDI. <https://www.freit.org/WorkingPapers/Papers/ForeignInvestment/FREIT130.pdf>
15. Bhargava, V., & Bolongaita, E. (2004). Challenging corruption in Asia: Case studies and a framework for action. The World Bank. <https://documents1.worldbank.org/curated/en/791211468741662651/pdf/275800PAPER0Challenging0corruption.pdf>
16. Fraud.com. (n.d.). Anti-money laundering (AML) – How it works and why it matters. <https://www.fraud.com/post/anti-money-laundering-aml>
17. Financial Action Task Force (FATF). (2021). Opportunities and challenges of new technologies for AML/CFT. FATF, Paris, France. <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/opportunities-challenges-newtechnologies-aml-cft.html>
18. European Central Bank. (2015). Virtual currency schemes – A further analysis. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemesen.pdf>
19. Financial Action Task Force (FATF). (n.d.). Virtual assets. <https://www.fatf-gafi.org/en/topics/virtual-assets.html>
20. Suprayitno, D., Sari, A. L., Judijanto, L., Amalia, D., & Sukomardojo, T. (2024). Blockchain and cryptocurrency: Revolutionizing digital payment systems and their implications on the digital economy. Migration Letters, 21(S6), 932-944. <https://www.migrationletters.com>
21. Hayek, F. A. (1976). Denationalization of money: An analysis of the theory and practice of concurrent currencies (Hobart Paper Special). Institute of Economic Affairs.<https://iea.org.uk/wp-content/uploads/2016/07/Denationalisation%20of%20Money.pdf>
22. Dyntu, V., & Dykyi, O. (2018). Cryptocurrency in the system of money laundering. Baltic Journal of Economic Studies, 4(5), 75–81. <https://doi.org/10.30525/2256-0742/2018-4-5-75-81>
23. Litvishko, O., Beketova, K., Akimova, B., Azhmukhamedova, A., & Islyam, G. (2020). Impact of the digital economy on the banking sector. E3S Web of Conferences, 159, 04033. <https://doi.org/10.1051/e3sconf/202015904033>
24. Drozd, O., Lazur, Y., & Serbin, R. (2017). Theoretical and legal perspective on certain types of legal liability in cryptocurrency relations. Baltic Journal of Economic Studies, 3(5), 221-228. <https://doi.org/10.30525/2256-0742/2017-3-5-221-228>
25. Claver, C., El Khoury, C., & Weeks-Brown, R. (2023). Financial crimes hurt economies and must be better understood and curbed. [https://www.imf.org/en/Blogs/Articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed#:~:text=Potential%20financial%20stability%20impacts%20include,trust%E2%80%94in%20governments%20and%20institutions](https://www.imf.org/en/Blogs/Articles/2023/12/07/financial-crimes-hurt-economies-and-must-be-better-understood-and-curbed#:~:text=Potential financial stability impacts include,trust%E2%80%94in governments and institutions)
26. Ministry of Foreign Affairs. (2023). National money laundering and terrorist financing risk assessment of Sri Lanka, 2021/2022 (Sanitized Report). <https://mfa.gov.lk/wp-content/uploads/2023/09/Full-Sanitized-NRA-Report.pdf>
27. Gunaratne, N. (2008). Golden Key: System and investors to blame, has the bubble burst at Ceylinco? Financial Times. <https://www.sundaytimes.lk/081228/FinancialTimes/ft306.html>
28. Kagan, J. (2023, December 17). What is Hawala? Money transfer without money movement. <https://www.investopedia.com/terms/h/hawala.asp>
29. Financial Action Task Force. (2024). Money laundering national risk assessment guidance. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Money-Laundering-National-Risk-Assessment-Guidance-2024.pdf.coredownload.inline.pdf>
30. The Morning. (2019, February 14). EU includes Sri Lanka in 'dirty-money' blacklist. The Morning. <https://www.themorning.lk/articles/22228>
31. Camacho, P. (n.d.). The road to money laundering centricity. <https://www.linkedin.com/pulse/road-money-laundering-centricity-paul-camacho>
32. Financial Action Task Force. (2010). Global money laundering & terrorist financing threat assessment: A view of how and why criminals and terrorists abuse finances, the effect of this abuse and the steps to mitigate these threats. <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Global%20Threat%20assessment.pdf.coredownload.pdf>
33. Financial Intelligence Unit of Sri Lanka. (n.d.). FIU establishment. Central Bank of Sri Lanka. <https://fiusrilanka.gov.lk/fiu_establishment.html>; International Monetary Fund. (n.d.). Core functions of an FIU. <https://www.elibrary.imf.org/display/book/9781589063495/ch03.xml>
34. Financial Intelligence Unit, CBSL. (2018). Guidelines for financial institutions on suspicious transactions reporting, No. 06 of 2018. <https://fiusrilanka.gov.lk/docs/Guidelines/2018/Guideline-06-2018.pdf>
35. Sunday Times. (2023, October 18). Central Bank fines four finance companies. <https://sundaytimes.lk/online/news-online/Central-Bank-fines-four-finance-companies/2-1143607>
36. Central Bank of Sri Lanka. (2024, November 26). Administrative penalties imposed by the Financial Intelligence Unit (FIU) on reporting institutions from May to October 2024. <https://www.cbsl.gov.lk/en/news/administrative-penalties-imposed-by-fiu-on-reporting-institutions-from-may-to-october-2024>
37. Financial Intelligence Unit of Sri Lanka. (n.d.). Legislation, rules and directions. Central Bank of Sri Lanka. <https://fiusrilanka.gov.lk/rules_directions.html>
38. Financial Intelligence Unit. (2023). Record-keeping requirements and practices in Sri Lanka. Central Bank of Sri Lanka. <https://www.cbsl.gov.lk/sites/default/files/cbslweb_documents/fiu/laws/Record%20Keeping_Requirements_Practices_SriLanka.pdf>
39. Financial Intelligence Unit. (2019). Guideline No. 01 of 2019. Central Bank of Sri Lanka. <https://fiusrilanka.gov.lk/docs/Guidelines/2019/Guideline-01-2019.pdf>
40. Financial Intelligence Unit. (2023). Guidelines on anti-money laundering and countering the financing of terrorism compliance obligations for attorneys-at-law and notaries, No. 02 of 2023. Central Bank of Sri Lanka. <https://fiusrilanka.gov.lk/docs/Guidelines/2023/Guidelines_02_2023.pdf>
41. International Monetary Fund & World Bank. (2004). Financial intelligence units: An overview. <https://www.imf.org/external/pubs/ft/fiu/fiu.pdf>
42. Ada Derana. (2024, July 25). During times of need, they chanted slogans without taking responsibility – President. <https://www.adaderana.lk/news.php?nid=100542>
43. Financial Action Task Force (FATF). (n.d.). FATF recommendations. <https://www.fatf-gafi.org/en/topics/fatf-recommendations.html>
44. Financial Action Task Force (FATF). (n.d.). Asia/Pacific Group on Money Laundering (APG). Retrieved from <https://www.fatf-gafi.org/en/countries/global-network/asia-pacific-group-on-money-laundering--apg-.html>
45. FT.lk. (2025, March 8). Sri Lanka prepares for key anti-money laundering evaluation ahead of global scrutiny. <https://www.ft.lk/front-page/Sri-Lanka-prepares-for-key-anti-money-laundering-evaluation-ahead-of-global-scrutiny/44-772916>
46. de Koker, L., Howell, J., & Morris, N. (2023). Economic consequences of greylisting by the Financial Action Task Force. Risks, 11(5), 81. <https://doi.org/10.3390/risks11050081>
47. Asia/Pacific Group on Money Laundering (APG). (2023, September 11). APG high-level delegation visits Sri Lanka. <https://apgml.org/members-and-observers/news/details.aspx?pcPage=1&n=5208>
48. ECONOMYNEXT. (2025, January 9). Sri Lanka’s anti-money laundering, terrorism financing evaluation postponed by 1 year. Retrieved from <https://economynext.com/sri-lankas-anti-money-laundering-terrorism-financing-evaluation-postponed-by-1-year-198840/>
49. **United Nations Office on Drugs and Crime (UNODC).** (2023, September). Sri Lanka: UNODC enhances policy engagement and partnerships to strengthen responses against drugs and organized crime. Retrieved from <https://www.unodc.org/southasia//frontpage/2023/September/sri-lanka_-unodc-enhances-policy-engagement-and-partnerships-to-strengthen-responses-against-drugs-and-organized-crime.html>
50. Davies. (n.d.). The role of cryptocurrency in money laundering. Retrieved from <https://www.daviescoin.io/blog/the-role-of-cryptocurrency-in-money-laundering>
51. Barr, M., Gifford, K., & Klein, A. (2018). Enhancing anti-money laundering and financial access: Can new technology achieve both? Retrieved from <https://www.brookings.edu/wp-content/uploads/2018/04/es_20180413_fintech_access.pdf>
52. McDowell, J., & Novis, G. (2001). The consequences of money laundering and financial crime. Retrieved from <http://usinfo.state.gov/journals/ites/0501/ijee/ijee0501.pdf>
53. Colombo Page. (2020). Sri Lanka: Transparency International warns of money laundering risks emerging from the government's "no questions asked" policy. Retrieved from <https://www.colombopage.com>
54. 54. Culp, S. (2015). Banks need strong, standardized anti-money laundering programs to fight financial crime. Retrieved from <https://www.forbes.com/sites/steveculp/2015/12/07/banks-need-strong-standardized-anti-money-laundering-programs-to-fight-financial-crime/?sh=3d8443a717a5>
55. 55. Huber, J.-A., Memminger, M., Soppitt, M., & Hayday, M. (n.d.). How banks can excel in financial crimes compliance. <https://www.bain.com/insights/how-banks-can-excel-in-financial-crimes-compliance/>