Challenges In Implementing AML Laws in the United Kingdom

Challenges In Implementing AML Laws in the United Kingdom

Introduction

A major threat to the integrity of the world economy and financial system is money laundering. Through a series of complex transactions, the introduction of illicit monies into the financial system, the concealment of their source, and the subsequent reintegration of the laundered money into the legal economy are the methods by which criminals attempt to legitimise the proceeds of their unlawful operations. Money laundering has far-reaching effects, such as making illegal activity easier, skewing financial choices, and undermining public trust in financial institutions. Anti-money laundering (AML) legislation and regulations are put in place by regulators in place to try to stop money laundering, however, there are still obstacles in the way of their successful implementation.

The implementation of anti-money laundering (AML) laws in the UK is hindered by persistent challenges, including human failures or biases in reporting suspicious transactions, inadequacies in customer due diligence (CDD) practices, and technological limitations in detecting money laundering activities. Despite the existence of robust legislative frameworks, financial institutions continue to struggle with issues such as delays or failures in reporting suspicious transactions due to human oversight or subjective judgments. Additionally, the reliance on automated systems for CDD and transaction monitoring presents technological challenges, including deficiencies in data accuracy and incomplete risk assessments. These challenges undermine the effectiveness of AML regulations, leaving financial institutions vulnerable to exploitation by criminals and facilitating the laundering of illicit funds. Addressing these issues is crucial for enhancing the integrity of the financial system and preventing the proliferation of money laundering activities.

The objective of this paper is to analyse the challenges in implementing Anti-Money Laundering (AML) laws in the UK, with a focus on issues such as delays or failures in reporting suspicious transactions, inadequacies in customer due diligence (CDD) and Know Your Customer (KYC) practices. This report concentrates on the UK's regulatory framework by defining money laundering and highlighting its significance, followed by an overview of AML laws and their evolution. The subsequent sections delve into specific challenges which are analysed in-depth, supported by relevant case studies and regulatory frameworks.

Money laundering

Money laundering is defined as “the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin so that they can be retained permanently or recycled into further criminal enterprises”. (Crown Prosecution Service, 2021). The consequences of money laundering are far-reaching and pose significant threats. To understand these implications better, it is essential to recognize that this process enables criminals to legitimise and benefit from the proceeds of illegal activities by hiding the origins of ill-gotten funds. Money laundering poses a severe threat to the integrity of the global financial system and economy at large. The money laundering process typically involves three stages: placement, where illicit funds are introduced into the financial system; layering, where the funds are transferred and disguised through complex transactions; and integration, where the laundered money re-enters the legitimate economy, appearing to have been derived from legal sources. The consequences of money laundering are far-reaching. It facilitates the perpetuation of criminal activities, distorts economic decisions, and erodes public confidence in financial institutions. Furthermore, the influx of laundered funds can destabilise housing markets, divert resources from essential services, and exacerbate socioeconomic inequalities.

Anti-Money Laundering

In response to the growing challenges posed by money laundering, governments and international organisations have implemented a robust regulatory framework to combat these activities. Anti-money laundering (AML) laws and regulations aim to prevent and detect money laundering by imposing stringent requirements on financial institutions and other regulated entities. AML laws have come a long way since its inception in late 1970. For almost thirty years, the UK has implemented legislation aimed at preventing money laundering activities. This legal framework governing AML efforts is comprehensive and continually evolving to address emerging threats.

Before Brexit, the UK adopted the European Union’s AML framework which comprised rules and regulations to combat financial crimes including money laundering and funding of terrorism by incorporating directives from the European Union. As a participant in the Financial Action Task Force (FATF), the UK has implemented most of the EU's six Anti-Money Laundering Directives (AMLDs) into its national law during its membership to comply with global standards.

Post Brexit, the UK is no longer bound by the EU's Money Laundering Directives (MLDs). However, it maintains alignment with international allies on Anti-Money Laundering (AML) strategies. The UK has adopted the Fifth Money Laundering Directive (5MLD) into its domestic law but hasn't opted into the Sixth Money Laundering Directive (6 MLD) yet *(The Law Society UK, 2021*). The European 4th Anti-Money Laundering Directive (4MLD) and the Funds Transfer Regulation were the subjects of the most significant current change, which took place in June 2017. Both regulations were influenced by a significant review of international standards in 2012.

The UK's AML landscape remains dynamic as efforts persist to strengthen regulatory frameworks and combat financial crime effectively. Major components in this framework are legislations such as the Proceeds of Crime Act 2002 (POCA), the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017), and the Terrorism Act 2000 (TA 2000). These laws alongside subsequent amendments provide the backbone for combating financial crime and ensuring compliance within the regulated sector.

AML Supervision

The Financial Conduct Authority (FCA) is the primary regulatory body responsible for overseeing AML compliance in the UK financial services sector. The FCA provides guidance and ensures that firms have robust systems and controls in place to mitigate money laundering risks. Apart from the FCA, other key supervisory bodies play crucial roles in overseeing AML compliance. For instance, the Prudential Regulatory Authority (PRA) which works by ensuring financial institutions maintain a strong risk management framework and implement effective controls to prevent money laundering. These two authorities collaborate closely to ensure comprehensive AML supervision.

Additionally, His Majesty’s Revenue & Customs (HMRC) plays a crucial role as a supervisory body for AML regulations as well as being a tax and customs authority. Globally, the Financial Action Task Force (FATF) is an intergovernmental organisation that sets international standards and promotes the effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, and other related threats to the integrity of the international financial system.

Despite these efforts, the fight against money laundering continues to pose significant challenges as described in the subsequent sections of this report. The Anti-Money Laundering (AML) laws were enacted primarily to combat terrorism, trafficking, fraud, and tax evasion. However, a key question arises: Are these legislations truly effective in achieving their intended purpose? Despite stringent laws and substantial fines, financial institutions continue to overlook transactions that violate these regulations, undermining their very purpose. Under the Money Laundering, Terrorist Financing, and Transfer of Funds (Information on the Payer) Regulations 2017 (MLR 2017), a Money Laundering Reporting Officer (MRO) is appointed who plays a crucial role. The MRO is responsible for reporting suspicious transactions to the National Crime Agency (NCA) through Suspicious Activity Reports (SARs). A Suspicious Activity Report (SAR) is a report making disclosures about the known or suspected transaction to the NCA about money laundering under Part 7 of the Proceeds of Crime Act, 2002 and terrorist financing under Part 3 of the Terrorism Act, 2000.

Section 330 of the POCA 2002, enshrines the responsibility of the employees of the regulated sector to report or disclose information to the NCA about any suspected transaction by way of a Suspicious Activity Report. It further entails that the person reporting the transaction must have reasonable grounds that another person is involved in money laundering. Section 331 of POCA, 2002, states that the person failing to disclose information as required under Section 330 of the Act would commit an offence under section 331 which may result in criminal prosecution. Despite having such robust legislation and rules, the UK legislation falls flat when it comes to implementation. A significant factor contributing to this challenge is the reliance on individual perception and choice in reporting suspected transactions. This approach not only leads to fragmented and potentially inconsistent identification of suspicious activities but also highlights varying levels of experience and ability among individuals to detect such activities effectively (Braithwaite & Makkai, 1994).

The challenges arising from human errors or biases in reporting suspicious transactions can be illustrated through cases such as the one involving Habib Bank AG Zurich. The Financial Service Authority (FSA), now FCA, fined Habib Bank and its former MLROs £525,000 and £17,500, respectively for failure to appropriately report high-risk customers and conduct enhanced due diligence before transactions occurring in the account, thereby violating the law.

(Final Notice Habib Bank AG Zurich, 2012) This case exemplifies how perceptions of high-risk customers and choices of due diligence can differ among individuals, and inadequate application can result in breaches of the law.

Another case, Regina *(The Financial Conduct Authority) Vs. National Westminster Bank Plc*, further underscores the consequences of implementation failures. NatWest was fined £264.8 million by the Southwark Crown Court for failure to conduct ongoing monitoring of the business relationship between itself and its commercial customer, Fowler Oldfield, a jewellery business. Although the agreement was that NatWest was not to manage or receive cash from Fowler Oldfield. £264 million out of £365 million deposited was in cash. NatWest failed to report the transaction as suspicious facilitating the laundering of this substantial sum. The Honourable Judge in this case opined that "it must be borne in mind that although in no way complicit in the money laundering which took place, the Bank was functionally vital. Without the Bank – and the Bank's failures - the money could not be effectively laundered". This case highlighted the importance of information sharing. Internal concerns about suspicious activity were not reported to authorities, allowing money laundering to continue.

The case of *Santander UK Plc* highlights the importance of up-to-date and ongoing transaction reporting and monitoring. In 2017, the FCA fined Santander £107 million for violating the regulatory obligations i.e., Money Laundering Regulations, 2007 and 2017 along with failure to maintain an effective AML framework. While Santander had an AML framework in place, its failure to continuously monitor transactions, conduct due diligence and update its systems led to ineffective implementation of this framework exposed by the FCA investigation. Santander's investigation unfurls the interconnected nature of the banking sector. In this case, Customer A is a business banking customer, whose banking activities did not trigger any high-risk alerts for the first five months initially. However, around October 2013, a considerable sum of money was deposited into his account. However, a suspicious transaction alert was triggered in November 2013 when the deposit exceeded £1.5 million within a month. This trend of transaction, although defined as medium risk, was not acted upon by the MRO for four months after which an investigation was conducted, and the recommendation was for the account to be closed. This recommendation was never implemented by Santander Bank as proven by a lack of supporting documents enabling Customer A to continue to launder money and commit financial crimes. The FCA while deciding on the case opined that delay and failure to act upon the investigator's recommendation was solely due to human oversight and lack of

formal procedure. The analysis of the Santander Bank case unfolds the challenges in the implementation of AML laws in the UK, frustrating the notion behind AML laws and regulations.

Santander's case throws light on the importance of the adoption of up-to-date and advanced technology in monitoring customer activities and how the use of this can be a game changer in money laundering detection and detection of violations of AML laws. Santander Bank had an automated transaction monitoring system which triggered alerts against specified rules. However, those rules did not consider vital customer information such as expected turnover, occupation, and nature of business of the customers. Consequently, the high-risk alerts for suspicious transactions were not triggered for its banking business customers as in the case of Customer A. The lack of sophisticated automated transaction systems made Santander's AML framework futile. (Final Notice Santander UK Plc, 2022) In 2017, Deutsche Bank AG was fined £163 million by the FCA for failure to detect, report suspicious transactions and keep up proper AML procedures between 2012 and 2015, violating POCA, 2002 and MRL, 2017 regulations.

The limitations of relying solely on technology for AML compliance are further highlighted by the case of HSBC Bank Plc (HSBC). While the Santander case exposed the shortcomings of inadequate transaction monitoring rules, HSBC's failings point to the broader issue of ineffective systems for detecting suspicious activity. HSBC Bank had a duty to maintain appropriate risk-sensitive policies and procedures as enshrined under the MLR, 2007, to identify, track and detect transactions showing colours of money laundering or terrorist financing, to validate that it is not being used for the purpose of financial crime. However, between 31 March 2010 and 31 March 2018 ("*the relevant period*"), HSBC failed to comply with the MLR, 2007. It failed to update the parameters of risks used to flag transactions as suspicious through its automated transaction reporting system. It neither fed the correct customer data nor updated its system which was used by its reporting system. These deficiencies resulted in a critical oversight. The bank failed to identify a customer involved in criminal activity, despite their account exhibiting suspicious activity. Notably, the customer received £127,000 spread across eighteen payments, a highly unusual pattern for someone declaring an annual income of only £40,000. This activity should have been flagged by the system in place to prompt further investigation, which unfortunately did not occur resulting in a £63.9 million by the FCA**.** (Decision Notice HSBC Bank Plc, 2021)

The financial institutions must update their frameworks with the evolving technology and complexity of the financial transactions. These slacked automated transaction systems do more harm than good. Other factors such as individual perception, choices in reporting suspicious transactions, and human oversights within financial institutions undermine the efficacy of these laws. High-profile cases involving Santander, NatWest, and HSBC illustrate instances where financial institutions failed to effectively implement AML regulations, leading to significant fines, and facilitating money laundering and financial crimes.

Customer Due Diligence

The effective implementation of customer due diligence (CDD) and Know-your-customer (KYC) measures is crucial for financial institutions to comply with AML laws and regulations. CDD and KYC procedures serve as the first line of defence against money laundering by preventing criminals from gaining access to the financial system. These procedures provide information to the financial institutions about the persons from whom they conduct transactions. Robust identification and verification processes make it more difficult for criminals to conceal their identities or the source of their illegally obtained funds. The purpose of KYC and CDD is to identify any risk-associated person, financial institutions are planning to onboard. (El Yacoubi, 2020).

Following the implementation of stricter regulations under the Money Laundering Regulations 2017 (MLR 2017), a high-profile enforcement action underscored the importance of comprehensive CDD practices and AML compliance. Regulated entities such as financial institutions and legal bodies must adhere to these rules and requirements set out to prevent money laundering and terrorist financing**.** However, these case studies demonstrate the potential pitfalls of inadequate AML procedures.

A major challenge is that several banks and financial institutions in the UK conduct international operations. These are large banks which have extensive global operations and complex corporate structures. This complexity can make it difficult to maintain a consistent and effective AML framework across all branches and subsidiaries. Ensuring that CDD and KYC processes are consistently applied and adhered to across all branches and subsidiaries can be an enormous task. As a prominent example**,** in 2019, the Financial Conduct Authority (FCA) imposed a significant civil penalty of £145,947,500 on Standard Chartered Bank (SCB) for

multiple breaches of the Money Laundering Regulations 2017. These breaches primarily occurred in the bank's UAE branches and the correspondent banking business within its UK wholesale banking segment. The FCA identified critical failures, including SCB's inability to establish and maintain risk-sensitive policies and procedures for customer due diligence, ongoing monitoring, record-keeping, and internal controls, breaching Regulation 20(1). As highlighted in the SCB's case, once a customer is accepted in one jurisdiction, the same customer could be offered products and services by SCB branches and subsidiaries in other jurisdictions. This meant that any AML control inadequacies in one jurisdiction had a profound impact on activities in others posing a significant challenge for maintaining consistent CDD and KYC standards across global operations. Also, regulatory compliance and control measures are often centralised at the head office level for these large financial institutions. This creates challenges in ensuring consistent implementation and oversight of CDD and KYC processes across all branches and subsidiaries, particularly in locations with varying regulatory environments or levels of AML/CFT risk exposure. (Final Notice SCB, 2019).

Building upon the Standard Chartered Bank (SCB) case, which exposed the challenges of maintaining consistent AML compliance across a global network, we now examine the Deutsche Bank case. This major German institution, with extensive UK operations, faced significant enforcement action by the FCA. Between 2012 and 2015, Deutsche Bank's Moscow branch was implicated in facilitating Russian money laundering activities in the UK through mirror trading. Deutsche Bank AG was fined £163 million by the FCA for failure to detect, report suspicious transactions and keep up proper AML procedures between 2012 and 2015, violating POCA, 2002 and MRL, 2017 regulations. These breaches highlighted major failings in Deutsche Bank's AML control framework within its Corporate Banking and Securities division. Deutsche Bank was found in breach of Systems and Controls (SYSC) rules 6.1.1R and 6.3.1 R, as the bank failed to conduct sufficient due diligence on the origin of funds and obtain sufficient information about its customers to inform the risk assessment process. The investigation exposed Deutsche Bank's deficient AML customer and country risk rating methodologies, deficient AML policies and procedures, and inadequate infrastructure that failed to provide a comprehensive repository of KYC information. Due in part to this deficiency, combined with the absence of automated AML systems for suspicious activity detection, Deutsche Bank was able to successfully transfer more than $16 billion out of Russia. Almost 2,400 mirror trades were made possible by the lack of automated procedures for

flagging suspicious transactions, which made it easier to move money secretly from Russia. (Final Notice, 2017).

Additionally, Deutsche Bank's complex management structures split responsibilities for AML compliance across multiple departments. This lack of clear ownership resulted in a lack of a sense of responsibility in its front-line staff for identifying and managing non-financial risks. These breaches violated the Financial Services and Markets Act 2000 and the Money Laundering Regulations 2007, which require financial institutions to establish and maintain an effective AML control framework proportional to the nature, scale, and complexity of their activities.

Another significant challenge arises from the need to tailor CDD and KYC processes to specific risk profiles of different customers and financial products. Some banking products or services present a higher risk of financial crime due to their inherent characteristics or the nature of the customer base they cater to. For example, private banking services for high-net-worth individuals or correspondent banking relationships with institutions in high-risk areas often require enhanced due diligence measures to adequately assess and mitigate the associated risks. Failure to tailor CDD and KYC processes to the specific risk profiles of different customers can leave financial institutions vulnerable. In the investigation into Guaranty Trust Bank (UK), GTBUK carried out by the FCA in 2013, the bank failed to review Politically Exposed Persons (PEP) and higher-risk customer relationships annually to ensure customer information was up-to-date and that the customer risk status was maintained appropriately and did not start the process of reviewing higher risk customer relationships until July 2010. This practice is in breach of principle 3 of the FCA's Principles for Businesses, Rules, and Guidance in the FCA Handbook. These deficiencies in the bank's AML practices which were in place for a significant amount of time pose a risk that customers have used the bank to launder the proceeds of crime. The bank's shortcomings were considered severe since a significant percentage of its customers are at higher risk and this served as a great entry point into the UK financial system for people from countries where money-laundering is more likely to occur. (Final Notice GTBUK Plc, 2013)

Finally, in recent years the introduction of new currencies such as cryptocurrency has changed the dynamics of the global financial industry. Cryptocurrency is a digital currency which uses cryptographic functions to have a safe and secure transaction. This digital currency offers a

wide range of benefits such as decentralisation and borderless transactions. Financial institutions scrutinise every transaction to flag any suspicious illegalities. However, the introduction of cryptocurrency has made it challenging to implement AML laws to ensure that the transactions undertaken using cryptocurrency are not for illegal purposes. The foremost challenge is that crypto facilitates cross-border transactions where different jurisdictions are involved leading to uncertainty and ambiguity. Some of the jurisdictions do not have strict laws for AML giving a safe passage to criminals to exploit them and launder money. *Simple Road: The Dark Web* exemplifies how cryptocurrency was used to undertake all sorts of illegal activities including money laundering.

With the increasing popularity of cryptocurrency and advancement in financial products, the regulators acted upon the need to bring it under the purview of law. The 5th Directive on Anti-Money Laundering included cryptocurrencies and other digital assets under the ambit of MLR, 2017. (Treasury, 2019) It included crypto assets exchange providers and custodian wallet providers in the 'obliged entity' and scope for the updated MLR, 2017. The inclusion bestowed the responsibility on the crypto exchange providers to conduct KYC and due diligence of every transaction. Do these inclusions help in the effective implementation of AML laws? It's still challenging. Cryptocurrency works on pseudonymity which means the person making the transaction is behind the veil of cryptographic addresses making it difficult for the financial institutions to conduct due diligence or KYC. Cryptocurrency is decentralised and works on Distributed Ledger Technology (DLT). The lack of central authority makes it challenging to effectively implement the AML laws and regulations.

Conclusion

Despite the UK's comprehensive anti-money laundering (AML) legal framework, significant challenges undermine the effective implementation of these laws and regulations. The cases examined in this report highlight crucial issues such as human errors and biases in reporting suspicious transactions, inadequacies in automated transaction monitoring systems, and difficulties maintaining consistent customer due diligence practices across global operations. Factors like individual subjectivity, technological limitations, and complex organisational structures have enabled major financial institutions to overlook evident money laundering activities.

The development of cryptocurrencies has added another level of complexity to the global financial sector because of its cross-border nature and fictitious transactions and also poses significant challenges in enforcing AML regulations.

Overcoming these hurdles will require a multi-step strategy involving enhanced employee training, substantial investments in advanced detection technologies, stringent regulatory oversight with severe penalties for non-compliance, and greater international cooperation. By addressing the human factors, technological gaps, and operational complexities discussed, financial institutions in the UK can sharpen their defences against money laundering, uphold the integrity of their financial system, and demonstrate their resolute commitment to combating financial crimes on a global scale. A collaborative approach involving financial institutions, regulators, law enforcement, and international partners is essential to surmounting the persistent challenges in implementing AML laws effectively.

Bibliography

Braithwaite, J. & Makkai, T., 1994. Trust and Compliance. An International Journal of Research and Policy, 4(1), pp. 1-12.

Crown Prosecution Service, 2021. Money Laundering Offences. [Online] Available at: https://www.cps.gov.uk/legal-guidance/money-laundering-offences.

Decision Notice HSBC Bank plc (2021).

Decision notice: Standard Chartered Bank 2019. Available at: https://www.fca.org.uk/publication/decision-notices/standard-chartered-bank-2019.pdf (Accessed: 01 March 2024).

ElYacoubi, D. (2020) 'Challenges in customer due diligence for banks in the UAE', Journal of Money Laundering Control, 23(2), pp. 527–539.

FCA Handbook: Financial Conduct Authority. Available at: https://www.handbook.fca.org.uk/.

FCA fines Deutsche Bank £163 million for serious anti-money laundering controls failings (2017) FCA. Available at: https://www.fca.org.uk/news/press-releases/fca-fines-deutsche-bank-163-million-anti-money-laundering-controls-failure (Accessed: 03 March 2024).

Final Notice Habib Bank AG Zurich (2012).

Final Notice Santander UK Plc (2022).

Final notice: Guaranty Trust Bank (UK) Limited. Available at: https://www.fca.org.uk/publication/final-notices/guaranty-trust-bank-uk-limited-2023.pdf (Accessed: 12 March 2024).

The law society: Anti Money Laundering after Brexit. Available at: https://www.lawsociety.org.uk/topics/brexit/anti-money-laundering-after-brexit