ISBN No: 978-99949-951-8-9

The challenging role of banks in preventing money laundering and terrorist financing

Goburdhun Kaushik

Introduction

From the Vienna Convention[1] to the implementation of the 4th EU AML Directive by European States, [2] banks are called upon to take increasing measures to prevent Money Laundering (ML) and Terrorist Financing (TF). Worldwide compliance costs incurred by financial institutions to prevent ML are estimated to have reached above USD 8 Billion in 2017.[3] J.P Morgan is reported to have invested billions of dollars and employed 13000 additional staff within compliance to meet its overall regulatory exigencies.[4] These costs trickling down to customers seriously risk vitiating the primary role of banks in providing affordable credit. Furthermore, inquisitive questioning during a routine Customer Due Diligence (CDD) exercise and temporary freezing of bank accounts, can seriously strain the relationship between banks and their customers.

Recent criminal and civil sanctions against banks for failing to take adequate measures to prevent money laundering and terrorist financing, have been a strong incentive for banks to reinforce compliance. The task of the bankers to identify suspicious transactions and make judicious decisions as to whether a red flag deserves to be raised to Financial Intelligence Units has become more complex and challenging.

---

[1] UN Convention against illicit traffic in narcotic drugs and psychotropic substances 1988.

[2] Directive 2015/849.

[3] PWC Global Economic Crime Survey 2016.

[4] Lin C.W.Tom, "Compliance, Technology and modern finance" BJCFCL 11 (Issue I) Fall 2016.

Nearly three decades after the establishment of the Financial Action Task Force (FATF), the time is ripe to reflect on whether international regulatory frameworks have lived up to their expectation in effectively combating ML and TF, and how costs of compliance can be curtailed, for Anti-Money Laundering (AML) and Combating Financing of Terrorism (CFT) regimes not to become "Too costly To Sustain" or "Too complex To Monitor."

1. The FATF

The FATF, an inter-government established in 1989, has as mandate the setting of standards and the promotion of effective implementation of legal, regulatory and operational measures, for combating ML and TF[5].

The FATF along with its nine FATF-styled regional bodies, oversee the implementation of FATF's forty recommendations, in over 190 jurisdictions. These recommendations not only comprise of preventive measures that financial institutions (FIs) need to implement but also require that these FIs be subject to adequate regulation and supervision.[6] By promoting harmonisation of regulatory as well as legislative frameworks, along with periodic mutual-evaluation of States, the FATF has set the stage to re-enforce the fight against ML and TF worldwide.

At the heart of this fight are banking institutions. Being custodians of financial information, they are vital sources of intelligence for law enforcement agencies (LEAs). Without their partnership, tracking illicit funds, understanding the pattern of terrorism financing, triggering investigations on financial crimes, confiscating assets and taking other sanctions as appropriate, against perpetrators or beneficiaries of financial crimes would be difficult, if not impossible.

[5] FATF Mandate 2012-2020.

[6] FATF (2012-2017) International Standards on combating money laundering and the financing of terrorism & proliferation.

2. The severity of sanctions & civil suits

Banks have been severely sanctioned for breaches of regulatory requirements relating to ML and TF. In the UK, the Financial Conduct Authority (FCA) expects compliance with the rules found in its handbook.

When Barclays failed to comply with its existing AML measures and entered into confidential agreements with its clients- that restricted its ability to carry out effective Enhanced Due Diligence (EDD)- the bank was held to be in breach of the FCA's principle 2, Principles of Business. The bank was found to have failed to conduct its business with due skill, care and diligence, notwithstanding the fact that there was no assertion that the funds emanated from any crime. The FCA fined Barclays £ 72, 069,400 (inclusive of a disgorgement of profit £52,300,000).[7]

Several other banks have been sanctioned by the FCA for not having adequate measures to prevent ML offences. Deutsche Bank was fined £163M, in January 2017 for breaching principle 3 of the FCA's Principles of Business, as well as for breaching other provisions found under the Senior Management Arrangements, Systems and Control. The bank had allowed a transfer of around USD10 Billion from Russia to offshore bank accounts, and that was highly suggestive of financial crime. It was found that Deutsche Bank (i) had deficient AML policies and inadequate CDD infrastructure, and (ii) used flawed customer and country rating methodologies.[8]

[7] Travers Smith RIG, "FCA and PRA enforcement actions: themes and trends" 2016 COB (136) 1.

[8] FCA Press release 31.01.17.

Furthermore, the FCA may rule that a person is not fit and proper for carrying out his functions, and thus prohibit that person from further exercising his designated functions. For example, when finding that the money laundering officer at Sonali Bank, had shown serious lack of competence and capability in carrying out his functions, the FCA fined him GBP 17900 and prohibited him from carrying out compliance oversight and money laundering reporting functions.[9]

The sanction regime in the United States is even more severe. In late 2012, HSBC entered into a deferred prosecution agreement with the United States Justice Department and agreed to forfeit USD 1.256 Billion for breaches of anti-money laundering provisions and pay USD 665M in civil penalties. The failure of AML controls at HSBC had facilitated money laundering of drug proceeds, worth USD 881M through the US financial system. As part of the deferred prosecution agreement, HSBC undertook to enhance its AML as well as its compliance obligations and effect structural changes within its entire global operations to prevent a repeat of the conducts that led to the sanction.[10]

Sanctions imposed upon banks can certainly cause loss of reputation and loss of business. The legal challenge of Bank Mellat against an order made by the UK Treasury on 9th October 2009, under Schedule 7 of Counter Terrorism Act (CTA) 2008 illustrates a long battle by the bank to winning back its reputation and recovering the losses that it incurred, because of a coercive application of the provision under the said anti-terrorism legislation. In fact, the order had required all persons operating in the financial sector, not to enter into or continue to participate in any transaction or business relationship with Bank Mellat, effectively shutting down the bank from the UK financial sector.

[9] FCA, Final Notice, Smith.S.G, 12.10. 16.

[10] US DoJ News, 11.12.12.

At first instance, Mitting J, at the High Court, held that, "the *objective of the order-to inhibit the development of nuclear weapons by Iran, is sufficiently important to justify interfering with property rights…In my opinion the risk of very great harm to vital national interest justifies the imposition of a severe and costly inhibition on the business of a bank which will entail long term damage to its goodwill in the UK.*"[11]The Court Appeal decision which upheld the judgment of Mitting J, was eventually overturned by the Supreme Court in 2013,[12] because (i) the singling out of Bank Mellat when other Iranian banks could potentially pose a similar threat to advancing Iran's weapons programmes was considered discriminatory, irrational and arbitrary, and (ii) the Treasury failed to give Bank Mellat an opportunity to make representations before the direction was issued. Bank Mellat is now suing the Treasury for damages in the tune of USD 4Billion[13].

The anti-terrorism regulatory landscape also makes banks more vulnerable to claims from victims of terrorist acts. This is well illustrated by the case of *Tziv Weiss et al v/s NatWest*.[14] The plaintiffs had suffered injuries or had family members killed, because of terrorist attacks perpetrated by Hamas, a terrorist organisation. The plaintiffs argued that NatWest provided banking services to a UK based charity Interpal, which was then supporting Hamas. Interpal was subsequently designated as a Specially Designated Terrorist by the US[15].

At first instance, summary judgment was granted in favour of the defendant bank. It was held that plaintiffs had no prospect in succeeding to prove, either that (i) NatWest had knowledge of Interpal's using the funds for financing terrorist acts, or (ii) NatWest exhibited deliberate

[11] Bank Mellat v HM Treasury [2010] EWHC 1332 (QB) paragraphs 16 and 20.

[12] Bank Mellat v HM Treasury (No2) [2013] UKSC 39.

[13] Rossington.R, Bank Mellat v HM Treasury, $4Bn Litigation slated for October, Lawyer Monthly, 12.09.16.

[14] US Eastern District Court of New York, 05-CV-4662, 28.03.13.

[15] Once so designated, banks should freeze assets of the said customer. See Executive Order 13224 made under the International Emergency and Economic Powers Act.

indifference, showing a substantial probability that NatWest was supporting terrorism by retaining Interpal's accounts or sending money at the behest of Interpal.[16]

The US Court of Appeals[17] overturned the judgment, hence allowing the plaintiffs to pursue with their claim. The court, after analysing the language of the terrorism offences under the US Codes, held that the test for a civil claim was not whether NatWest employees had knowledge of Interpal's terror financing, but whether they had knowledge of Interpal financing a terrorist organisation. On the issue of there being no evidence that NatWest was indifferent to supporting terrorism, the court went on to hold that the lower court had placed too much reliance on the findings of the UK charity commission which concluded that there was no evidence of Interpal financing Hamas political and violent military activities. The correct issue- according to the appellate court- that ought to have been considered, was whether Interpal provided support to Hamas regardless of purpose.

The subtle differences in the reasoning of the courts, which tilts the balance in favour of the plaintiffs, opens a floodgate of potential claims for extracting compensation from the banking sector and would most certainly be a cause of concern for banks.

Banks should also be alive to potential criminal sanctions or of statutory obligations to act in a specific manner. Under the UK Terrorism Act (TA) 2000, for instance, criminal sanctions are provided for persons, who despite suspecting or having reasonable grounds to suspect, that (i) funds are being raised for terrorism financing, (ii) money or other property are being used for the purposes of terrorism, or (iii) funding arrangements have been entered for the purposes of terrorism, actually fail to disclose these transactions to the competent

[16] US Eastern District Court of New York, above n.14.

[17] US Courts of appeal, 2nd Circuit 13-CV-1618, September 22, 2014.

authorities.[18] It is also an offence for a person to enter funding arrangement when there are reasonable grounds to suspect that funds may be used for the purpose of terrorism.[19] Once a disclosure has been made to the authorities, the bank will not be able to deal with the funds, unless it is so duly authorised by the authorities.[20]

3. What does Compliance entail?

Banks must (i) establish clear responsibilities to ensure that policies and internal controls are introduced and maintained which deter criminals from using their facilities for ML and TF, (ii) have sound "Know Your Customer" (KYC) procedures in place to be able to identify the true identity of their customers before opening any account to reduce the likelihood of them being used as vehicles for laundering the proceeds of criminal activities or moving terrorist funds. For instance, as it is increasingly recognised that terrorist groups are having recourse to clubs and charities, banks should ascertain the legitimate purpose of these organisations and should establish the identity of the persons who are in control of these clubs and charities. With respect to trusts, banks would require as minimum information, the name of the trust, proof of its existence, its address, country of establishment, as well as names of the settlor, beneficiary, protector (if any) or class of beneficiaries, and any other natural person exercising ultimate effective control over the trust.[21]

Banks should also be able to (i)develop a thorough understanding of ML/TF risks present in its customer-base, products, delivery channels, services, and jurisdictions with which they or their customers do business, (ii) design and implement policies for customer acceptance, due

[18] For similar provisions in the US, see Title III Patriot Act.

[19] S 17 TA 2000. See also s14 & 15 of the Prevention of Terrorism Act (PoTA) 2000, in Mauritius.

[20] Section 21ZA, TA 2000. See S 2239B(a)(2) of the US Code,which creates a legal obligation for Financial Institutions (FIs) to retain control and possession of any funds in which a foreign terrorist organisation or its agent has an interest. The FIs should also report to the authorities the existence of such funds.

[21] Bank of Mauritius, Guidance Notes on Anti-Money Laundering and Combating the fInancing of Terrorism, updated as at July 2017.

diligence and effect ongoing monitoring to adequately control ML/TF risks, (iii) carry assessment of ML/TF risks, of not only an individual customer but also at an enterprise wide level..[22]

Banks need to (i) keep proper records – including identity and transaction records- to allow for an effective audit trail; for instance, with respect to wire transfers, the names of the originator and beneficiary should be clearly identified, (ii) carry ongoing monitoring of accounts and transactions, (iii) file suspicious activity records when required, and (iv) provide ongoing training to their staff to discharge their statutory duty for taking appropriate measures to prevent their services from being used to launder money or for terrorist financing. [23]

In the UK, banks are expected to comply with the Money Laundering, Terrorist Financing and Transfer of Funds (information of the payer) Regulations (MLR2017) which implement the 4th EU AML Directive. MLR 2017 bring some notable changes when compared to the repealed Money Laundering Regulations of 2007 (MLR 2007). Under MLR 2017, when adopting a risk-based approach,[24] financial institutions will henceforth need to formally communicate their risk assessment to their supervisory authorities.[25] Transactions for which Enhanced Due Diligence (EDD) needs to be carried out, would take into consideration criteria falling under three categories namely: (i) customer risk factors (ii) product, service or delivery risk factors, and (iii) geographical risk factors.[26] UK Politically Exposed Persons

[22] Bank of Mauritius, Guidance Notes, above n.21.

[23] Bank of Mauritius, Guidance Notes, above n.21.

[24] The FATF also recommends that banks and supervisors adopt a risk-based approach to assess ML and TF risks. In essence, resources are to be deployed in an effective way to focus more on areas of high risks and thus curtail ML and TF risks, where they matter most. See FATF, Guidance for a risk-based approach:The Banking Sector (Oct 2014).

[25] Reg 18(6) AMR 2017.

[26] Annex 3, 4th EU AML Directive 2015/849 & Reg 33 AMR 2017.

(PEPs) and those of the European Economic Area, will now be subject to EDD. Furthermore, compliance officers will henceforth need to take into consideration far more factors before determining whether a transaction is of low risk, to justify the carrying out of simplified due diligence.[27]

Manoeuvring through the procedures to comply with AML requirements might be complex enough, but banks are also called upon to prevent TF. They will, for that purpose, need to be vigilant to the orders issued by international organisations and the executive, to refrain from dealing with property held by a designated terrorist or designated terrorist organisations.

For instance, in the UK, banks should also be attentive to actions that can be taken by the Treasury. Under the Anti-Terrorist Crime and Securities Act (ATCSA) 2001, the Treasury may apply for freezing orders and thus prevent funds from being made available to persons named in the order.[28] Under Schedule 7 of the Counter-Terrorism Act (CTA) 2008, banks may be given directions by the Treasury to carry customer due diligence, ongoing monitoring, systematic reporting, or to limit/cease its business with a customer. Banks can also be required by the Treasury under the Terrorist Asset Freezing etc (TAF) Act 2010, not to make economic resources available to, or to the benefit of, persons/entities- designated by the Treasury- when it reasonably believes that they have been involved in a terrorist activity. Banks/Bankers should, if they are not to be prosecuted for having committed an offence,[29]be vigilant of who are on the consolidated list of targets[30] which is regularly updated by the

---

[27] Reg 37 AMR 2017.

[28] In Mauritius, the Minister to whom the subject of National Security is assigned may declare a person to be an international terrorist, and cause a public notice to be published, subsequent to which the Bank of Mauritius may direct that any account, property or funds of these persons be frozen. See Section 10(7) of PoTA and Regulation 3 of the Prevention of Terrorism (Special Measures) Regulations 2003.

[29] Paragraphs 30-30A, Schedule 7, CTA 2008.

[30] See HM Treasury, Financial Sanctions: Consolidated list of targets.

Treasury. They have a legal obligation to freeze assets of these targets and deprive them of financial services.

Furthermore, banks in UK should note the functions of the Office of the Financial Sanctions Implementation (OFSI), established in March 2016, which aims to detect, respond to and address breaches of financial sanctions, that have been imposed by the United Nations Security Council, the EU Financial Sanctions Regulation, or under the UK domestic legislations such as under the ATCSA 2001, CTA 2008 or TAF 2010.

Guidelines issued by the Basel Committee on Banking Supervision states that terrorism has its own specificities and that financing can come from legal sources. This can make it difficult for the banker to make a value judgment as to whether a transaction is suspicious. The said Guidelines, further states that CDD, as applicable for detecting ML offences should help a bank to detect and identify potential TF activities.[31] In order to build their skills to identify a potential transaction relating to TF and make a suspicious activity report when appropriate, bankers are further called upon to learn, from published FATF reports, terrorist financing methods and techniques.[32]

4. Criticisms of the AML/CFT Regime

(a) As highlighted above, staggering costs is a prime concern. Sathye[33] argues that increasing costs of compliance could (i) decrease capital available to banks to support lending, (ii) increase cost of credit which would entail fewer people having access to credit facilities, (iii) from a broader business perspective, affect competitiveness of an economy, and (iv) oblige

[31] Guidelines on "Sound management to risks related to money laundering and terrorist financing" (June 2017), para 59-61.

[32] Bank of Mauritius, Guidance Notes, above n.21.

[33] See Sathye.M, Estimating the cost of compliance in AMLCFT for financial institutions in Australia" (2008) JFC 15(4) 347.

smaller financial institutions that cannot readily absorb the increased regulatory costs to undergo structural changes to survive or risk going out of business. Furthermore, there is no tangible proof that compliance costs have provided commensurate benefit to society.

(b) Identification of a suspicious transaction and raising of a Suspicious Activity Report (SAR) is at the root of the fight against ML/TF. Tákats[34] notes, that there has been an explosion in the number of SARs filed with the US Financial Crime Enforcement Network (FinCEN) over a ten years' period. He opines that excessive reporting is consonant to a diminution in information value being imparted to government agencies. The "crying wolf" syndrome means that banks, without applying a reasoned approach, would too readily report transactions, over and above those that would truly qualify as suspicious. But can we blame the banks from adopting such defensive attitude? Certainly not, if we consider the severity of sanctions that can be imposed and the fact that the duty to report arises upon mere suspicion or upon having reasonable ground to suspecting that ML could be taking place.[35]

(c) Goldby[36] is critical with respect to the usefulness of SARs. She refers to the fact that, (i) a high proportion of SARs are disseminated to tax authorities and not to Law Enforcement Agencies (LEAs), thus SARs are not playing the expected role of combatting organised crime, (ii) despite criminal prosecution for money laundering is on the rise, there is not enough statistics to demonstrate that these prosecutions were as a result of investigations arising from SARs, and (iii) although the FATF considers the number of prosecutions and convictions obtained along with the amount of assets seized, as a measure of effectiveness of

[34] Tákats.E, "A theory of "crying wolf": The economics of money laundering enforcement" 2011 JLEO, 27(1), 32.

[35] Ahmad v HM Advocate 2009 HCJAC 60.

[36] Goldby. M, "AML reporting requirements imposed by English Law: measuring effectiveness and gauging the need for reform", 2013 JBL (4), 367.

reporting systems, the said measure fails to balance the costs of implementing the reporting systems with respect to outcomes.

(d) Twenty years ago, it was estimated that funds laundered worldwide were already anything between USD 590 Billion to USD 1.5 Trillion.[37] It is currently estimated that 100 Billion GBP is laundered every year in the UK alone.[38] After more than a decade of rigorous application of AML regime worldwide, one would legitimately expect that the value of confiscated property would have reflected those estimates. But quite the contrary, the UK National Audit Office, seriously puts into doubt the effectiveness of confiscation orders under Proceeds of Crime Act by indicating that only 26 pence out of every £100/- of criminal proceeds are being confiscated.[39]The number of mutual legal assistance requests from foreign governments to UK authorities has however increased by 12% in a year, indicating that despite banks' controls, ML through the banking system has become increasingly easy to disguise.[40] As the estimates of global proceeds of illicit funds[41] are overwhelmingly well above the amount of funds being confiscated and forfeited,[42] it would seem that AML provisions are porous and have not stopped criminals in benefitting from proceeds of crimes.

(e) Increased compliance costs and the risk of being heavily fined, have prompted several banks, under a risk-based approach, to de-risk their banking activities or more literally to de-bank those customers that they feel may pose a higher risk. The President of the FATF has

[37] Tanzi, "Money Laundering and the International Finance System," IMF Working Paper No. 96/55 (May 1996).

[38] House of Commons, Home Affairs Committee, "Proceeds of crime" 5th report of session 2016-2017 (HC25).

[39] Ibid.

[40]Binham.C, " Foreign Money Laundering inquiries to UK leap 12%" Financial Times 11.06.17.

[41] US National Money Laundering Risk Assessment 2015, estimates global illicit proceeds to USD 300 Billions.

[42] In 2015, total assets owned by the US government in its Assets Forfeiture Fund amounted to USD 6,513 Million. See Audit of the Assets Forfeiture Fund and Seized Asset Deposit Fund, Annual Financial Statements 2015, at page 6.

been highly critical of banks' manoeuvres to de-risk and emphasised that at no time has the FATF condoned such practice. What the FATF requires is for banks to conduct proper analysis, quantify what the risk is and take calibrated actions.[43] Yet, banks have adopted an excessively cautionary approach, with the net effect that numerous money service businesses, foreign embassies, international charities and correspondent banks have had their bank accounts closed or have been denied banking services. In an era, where financial inclusion is considered as a means to reducing poverty and encouraging economic development, large communities are increasingly being left out of the banking sector.[44]

(f) Further evidence of how the bank-customer relationship has taken a back seat, can be illustrated from the application of AML legislation in the decision reached by the chancery court in *Squirrel v/s National Westminster Bank and anor.*[45]In the said case, Squirrel found itself subject to an investigation by the HM Customs and Excise for value added tax. The bank froze its account which was some £200 000 in credit. The bank could not explain to the customer the reason behind its own act, because that would amount to the offence of tipping off, and it could not give effect to the instructions emanating from the client as allowing any transfer without the consent of the relevant authorities- which ought to be communicated within a prescribed statutory delay-would also have constituted an offence. The court found the conduct of the bank to be unimpeachable, and held that even if Squirrel was innocent, the bank would not be liable to compensate Squirrel for its loss. In other words, the court expects compliance with the AML regime, notwithstanding the fact that this may jeopardise the relationship between a bank and its customer.

[43] Arnold.M, " FATF warns on banks' approach to de-risking," Financial Times 13.11.2014.

[44] Durner.T and S.Liat, " Understanding bank de-risking and its effect on financial inclusion" Research Report November 2015.

[45] 2005 EWHC 664.

(g) If a banker overcomes the difficulty of understanding what amount to terrorism, he/she may be wary to understanding how regulations that are applicable to money laundering would be of assistance to fighting TF. AML regulations seek to link money, which is either entering, already within or leaving the financial system, to a crime. CFT seeks to connect information about existing terrorism activity to money in or leaving the financial system. Thus, for a banker to be able to consider whether a SAR ought to be raised, he will potentially need to form the view that the beneficiary of the funds is connected to terrorist activities. Gilmour[46] opines that AML practices would be hard pushed to detect money transferred for terrorist financing, unless the amounts were sufficiently high and were aligned to factors that would normally have raised a red flag.

(h) The attack on the World Trade Centre in September 2001 met with prompt action from the United Nations and under UN resolution 1373, countries were called upon to (i) prevent and suppress the preparation and financing of terrorism, (ii) criminalise wilful collection of funds which would be used to carry out terrorist acts, and (iii) freeze without delay the assets and economic resources of persons and entities who commit, attempt to commit, or facilitate the commission of terrorist acts.

The concept of how terrorism had been addressed in international instruments evolved from one, whereby States considered themselves to be victims, to one where they regard themselves as being the protectors of the common good. Consequently, for States to be successful in preventing terrorism, they had to go beyond mere criminal prosecution or

[46] Gilmour.N, "Examining the practical viability of internationally recognised standards in preventing the movement of money for the purpose of terrorism." 2017 JFC, 24(2), 260.

maintenance of peaceful inter-state relations, and look to regulatory response. Financial institutions became frontline enforcers of international norms alongside state organs.[47]

Following the 2001 attack on the World Trade centre, the FATF was prompt to issue further recommendations relating to terrorism financing. These not only embodied the aims under UN Resolution 1373 but financial institutions and other businesses were also required to report promptly to competent authorities, their suspicion that funds were linked or related to, or were to be used for terrorist acts or by terrorist organisations.[48]

It is estimated that carrying out the September 11th attack on the World Trade Centre costed about USD 300,000 and even if that transaction had been identified in the banking circuit, it would have been difficult for any Law Enforcement Agencies (LEAs) to determine the illicit use that would have been made of the funds.[49] A further argument which is made to sustain that AML regulations are not fit for combatting financing of terrorism, is crafted by looking at how the recent terrorist attacks occurred and query whether their financing would have warranted a banker raising a red flag, in the first place. The terrorist attack at London Bridge in June 2017 which killed eight people and injured dozens more, only costed the price of hiring a van, which was used to run down pedestrians.[50] Heike Mai, Deutsche Bank economist, is reported to having stated that an analysis of 40 jihadists attacks in Europe in the past 20 years, showed that most of the funding for the attacks derived from the terrorists' own

[47] Ali.T.N " Dynamism and the erosion of procedural safeguards in international governance of terrorism" Thesis September 2015

[48] FATF IX Special Recommendations, October 2001.

[49] Davis, "The financial war on terrorism" in Ramraj & others, "Global Anti-Terrorism Law and Policy" 2nd Edition, 2012, (CUP), 205.

[50] BBC News, "London bridge attack" 09.06.17.

funds and that 75% of these attacks costed less than USD10,000 and would not have raised any SAR.[51]

5. Addressing the Criticisms

Maintaining integrity and stability within the financial sector, requires strong rules for banks to prevent their services from being used to launder money and for financing of terrorism activities. It would be wrong to brush aside the fact that SARs have been ineffective in combatting financial crimes. Indeed, although there are certain jurisdictions which are not transparent with respect to how many SARs led to investigations and prosecutions, others are. FinCEN, for instance, publishes on its website a series of enforcement actions taken, following receipt of SARs. FinCEN values SARs, and even holds an annual law enforcement awards ceremony to present awards to LEAs which had made use of reports emanating from financial institutions under the Bank Secrecy Act to trigger investigations that resulted into criminal proceedings being initiated.[52]

Furthermore, defensive reporting which might have accounted for high number of low quality SARs may not be acceptable anymore. According to UK National Crime Agency's "Guidance on submitting better quality SARs"- published in September 2016- it can be gathered that the grounds for suspicion or reasonable grounds to suspect, that a specific predicate offence had taken place, needs to be stated explicitly within the SAR, leaving no room for any guess work from the reporting officer. In essence, banks are being guided on how they should more effectively raise an SAR, if at all.

[51] Martin.W, "One chart shows how little it costs terrorist groups like ISIS to carry attacks in Europe" Business Insider UK, 02.12.16.

[52] FinCEN News release, "Awards Recognize Law Enforcement Success Stories Supported by Bank Secrecy Act Reporting" May 2017.

As the probability of a banker to identify whether funds are linked to terrorist financing is minimal, it is tempting to argue that, attempts to prevent TF and the accompanying regulatory approach ought to be abandoned. But such an argument would translate a misunderstanding of the theory of risk management and how such theory influenced regulation to prevent terrorism.

Renn[53] states that, in the twenty-first century, focus had shifted from minimizing or reducing risks, to increasing resilience against the unforeseen, by adopting a preventive approach to risk. Analysing what a preventive approach entails, Aradau notes that, as low probability/high consequence catastrophes will happen in the future, any level of risk is unacceptable. A potential threat is to be curbed, not on the basis of what is known, but on the basis of the unknown.[54] The requirement for filing SARs with respect to potential terrorist financing transaction falls within the ambit of the preventive principle to managing unpredictable risks.

One cannot underscore enough the nexus between criminal activities and terrorist financing. A FATF study, in five western African countries demonstrates that terrorist groups obtained funding from drug and human trafficking, extortions, robberies and so forth.[55] The Islamic state of Iraq and al-sham (ISIS) a terrorist organisation in the Middle East is reported to be funding itself from bank robberies, looting, but mainly from smuggling of crude oil from Iraq and Syria to regions in Turkey and Iran.[56] This illustrates the fact that the use of SARs can potentially raise red flags with respect to supected ML offences. Ensuring investigations may then disrupt financial flows to terrorists.

---

[53] Renn.O, "Risk Governance-Coping with uncertainty in a complex world" (earthscan) 2008, 193.

[54] Aradau.C, "Governing Terrorism Through Risk: Taking Precautions, (un)knowing the Future" (2007) EJIR,13(1) 89

[55] FATF Report: " Terrorist Financing in West Africa" October 2013.

[56] Pollock-Brooks.T, "Paris attacks: Where does ISIS gets its money and weapons?" The Independent, 16.11.2015.

There is also a misconception that a regulator will too readily adopt a deterrent policy which, is confrontational, sanctions rule-breaking behaviours, is adversarial in nature and which focuses on guilt establishment. Applying a deterrent policy outright may not buy-in a conducive attitude for stakeholders to comply with regulation. Regulators seem to have embraced a practical approach when applying enforcement strategies. The Enforcement Guide (EG) of the FCA in the UK, states that the effectiveness of the regulatory regime depends to a significant extent on maintaining an open and co-operative relationship between the FCA and those it regulates.[57] Regulators having proactive risk-based supervision and monitoring approaches, will in some cases where contraventions have taken place, decide not to take any disciplinary action, but will expect firms to prompt remedial steps, when regulatory breaches are identified.[58]

In determining whether to take action such as financial penalty or public censure, factors such as (i) nature, seriousness and impact of the suspected breach, and (ii) conduct of the person after the breach,[59] will be taken into account. The breaches of various requirements imposed upon banks under MLR 2017 to combat ML and TF, can be sanctioned civilly or by means of criminal prosecution.[60] The FCA's Enforcement Guide states that criminal prosecutions will be undertaken where appropriate and when they meet the supervisory authority's statutory objectives.[61] A practical approach to enforcement therefore allows for flexibility, in taking sanctions commensurate with the seriousness of the breach.

[57] E.G 2.1.2(1).

[58] EG.2.1.4.

[59] FCA, Decision Procedure and Penalties (DEPP) manual.

[60] Part 9, MLR 2017.

[61] EG 12.1.1 and 12.1.2.

However, although regulators may take a practical approach to promote compliance, banks always risk in being severely sanctioned for regulatory breaches. This explains their heavy investment in compliance. Mugarura, argues that AML rules relating to customer due diligence are onerous and banks should be compensated by means of tax rebate,[62] if they have strong measures to combat money laundering. Such a proposal would be hard to sell, especially when in the wake of the global financial crisis, confidence in banking institutions took a nose dive. The subsequent crisis in UK, relating to mis-selling of interest rate hedging products, manipulation of LIBOR, payment of excessive remuneration and so forth, have not helped in convincing the public or legislators that banks are qualified for a tax rebate on that score.

Conclusion

We do not live in a utopian world, where human greed is non-existent, and values of good governance prevail unfailingly. Combating ML and TF should be relentless and necessary. Over the past decades, States, regional and international organisations have contributed to making the AML/CFT regime more robust to maintain integrity and stability within the financial sector. To that end, significant costs have been incurred.

In light of the fact that there are no signs of regulatory abatement, a balance needs to be struck between on the one hand, the functions of banks as profit making entities and on the other hand, the requirement for banks to act for a common good, namely that of preventing their services from being used for unlawful deeds.

Since 2016, the FCA has taken several initiatives to lower cost of compliance. Firms have been asked to develop and adapt new technologies that can make regulatory reporting and

[62] Mugarura.N, " The jeopardy of the bank in enforcement of normative anti-money laundering and countering financing of terrorism regimes," 2015 JMLC 18(3) 352.

interpreting FCA's handbook, more economical, efficient and effective.[63] Furthermore, consideration is being given to proposals to allow firms to share and discuss information on customers. Firms will thus be able to make informed decisions as to whether suspicion is warranted, thus reducing the number of defensive SARs filed and the costs attributed to them. A proposal for a centralised platform to monitor transactions has been made to assist both FIs and LEAs to identify financial crimes. The FCA further proposed that FIs should be able to rely on third party due diligence, effectively cutting a red-tape, and allowing a customer to enter a business relationship more easily.[64]

But will we be witnessing a fall in the cost of compliance soon? In February 2018, the Monetary Authority of Singapore issued new guidance to financial institutions on the use of innovative technology solution to facilitate safe, non-face-to-face customer onboarding. To detect and deter ML and TF, and safeguard against self-personification, financial institutions in Singapore, make use of biometric identification, real time video conferencing and use of secure digital signature.[65] With the current trend, Fintech Firms are bound to come with innovative solutions, in the coming years, to capitalise on the need to curb compliance cost in the banking sector.

[63] FCA Business Plan 2017-2018, 44.

[64] FCA Anti Money Laundering Annual Report 2016, 15-16.

[65] See http://www.mas.gov.sg/News-and-Publications/Media-Releases/2018/MAS-Encourages-Financial-Institutions-to-Use-Technology-to-On-Board-Customers-More-Efficiently.aspx

Bibliography

Aradau Claudia and Munster Van Rens, "Governing Terrorism Through Risk: Taking Precautions, (un)knowing the Future" (2007) European Journal of International Relations,13(1) 89

Baldwin Robert, Cave Martin, and Lodge Martin, "Understanding Regulation- Theory, strategy and Practice" 2nd Edition, OUP, 2012

Cheung Rita, "Money Laundering-a new era for sentencing organisations" 2017, Journal of Business Law (1), 23

Croucher Shane,"Western Banks, Terrorism and Isis, The Nihilism of Dark Finance Fuelling Global Insecurity", International Business Times, 03rd March 2017, at http://www.ibtimes.co.uk/western-banks-terrorism-isis-nihilism-dark-finance-fuelling-global-insecurity-1474508

Cuellar Mariano-Florentino, "The tenous relationship between the fight against money laundering and the disruption of criminal finance" (2003) Journal of Criminal Law and Criminology, 93(2) 311

Elder Shaun,"Sanctions and financial regulation: a mediation upon "natural necessity" (2013) Dublin University Law Journal, (36), 217.

Etienne Julien, "Ambiguity and relationship signals" (2013) Journal of Regulation and Governance, 7(1)30

Gilmour Nicholas, "Examining the pratical viability of internationally recognised standards in preventing the movement of money for the purpose of terrorism." (2017) Journal of Financial Crime, 24(2), 260.

Goldby Miriam " A reporting requirements imposed by English Law: measuring effectiveness and gauging the need for reform" (2013)Journal of Business Law, (4)367

Lin C.W.Tom " Compliance, Technology and modern finance" – Brooklyn Journal of Corporate Finance & Commercial Law (BJCFCL) Vol. 11 Issue I Fall 2016

Mugarura Norman, " The jeopardy of the bank in enforcement of normative anti-money laundering and countering financing of terrorism regimes" (2015) Journal of Money Laundering Control 18(3) 352

Nielsen Lehmann and Parker Christine, " Testing responsive regulation on regulatory enforcement" Regulation and Governance (2009),3(4) 376.

Parker Christine, " Twenty years of responsive regulation: An appreciation and appraisal" (2013) Journal of Regulation and Governance, 7(1) 2.

Renn Ortwin, "Risk Governance-Coping with uncertainty in a complex world" (earthscan) 2008

Roopanand Amar Mahadew, "The Good Governance and Integrity Reporting Act 2015" Mauritius legislates once more on corruption. Statute Law Review (2017) 38(2) 170

Sathye Milind, " Estimating the cost of compliance in AMLCFT for financial institutions in Australia" (2008) Journal of Financial Crime, 15(4) 347

Srivastava Arun, Simpson Mark, Moffatt Nina, Powell Richard, and Foster Isabel, "Financial Crime Update"(2017), Compliance Officer Bulletin (147), 1

Tákats.E " A theory of "crying wolf": The economics of money laundering enforcement" Journal of Law, Economics and Organisations (2011) 27(1) 32

Travers Smith Regulatory Investigations Group, " FCA and PRA enforcement actions; themes and trends" (2016)Compliance Officer Bulletin (136),1.