Law and finance: money launderings laws cdd

Economics, Money

Executive Summary

In the recent times, new and innovative methods of funds transfer through electronic methods across the borders have increased. These have opened new opportunities formoneylaundering and financing ofterrorism. With the recommendations made by the FAFT that the principle of Customer Due Diligence (CDD), conducted by financial institutions, be set out in law, a robust CDD system would be of paramount importance for financial institutions in the UK should FATF's recommendations be implemented in the UK. Owing toglobalizationof businesses, a recommendable CDD team should comprise of human resources specialists, IT experts, law experts, financial experts, representatives in various countries along with functional area managers with a good understanding of various cultures. This would bring about effectiveness and efficiency in the application of CDD measures in the current world with the increased use of New Payment Methods. As such, a firm wishing to provide NPM as one of its services or products should ensure that it has the CDD team in place with various expertise.

Introduction

Recently, economics has witnessed money laundering alongside the issue of the financing of terrorism, among other issues. In correspondence to this point, the United Kingdom has played a key role in the international fight against money laundering through anti-money laundering (AML) legislation which has been made possible through the impetus of international organizations such as the Financial Action Task Force (FATF). As recently as February 2012, the FATF recommended that the principle of Customer Due

Diligence (CDD), conducted by financial institutions, be set out in law. This was advocated in the recent FATF report “ International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation” published in February 2012. The following is a report by the head of AML at a large financial services firm, which advised the company’s board on the ‘ perfect model’ for a robust system of CDD in order to ensure compliance should FATF’s recommendations be implemented in the UK.

Analysis of the objectives of an effective system of CDD and what it should contain

The term ‘ robust’, when used in this context, implies that the CDD system in question should possess an ability to effectively perform its function even when its assumptions or variables are misrepresented. The CDD model to be implemented should work effectively, withoutfailure, in a diversity of circumstances and as such, it should not conflict with the law. As such,

A perfect CDD system should contain tight and secure quality controls
There should be effective policies, processes and procedures in place to ensure compliance with the regulatory requirements in the global arena
Effective protective mechanisms should be put in place
It should be cost effective –maximising on benefits while minimising costs.
A perfect CDD system should be risk-sensitive
Adoption of procedures such as ‘ know-your-customer’, should be adopted within individual Jurisdictions
Guidelines for the resolution of issues should be put in place should information made be inaccurate or insufficient.
It should be strict and as such in compliance with the legislative laws

It should be technologically competent given that the market is currently dominated by New Payment Methods which needs one to be technologically savvy

Contents of a Robust CDD System

A robust CDD system that can work in the current market described by high competition from the globe,

Should contain human resources specialists with a strategic view of the particular organization since there is much competition from the international market.

There should also be functional area managers in possession of technical expertise and the ability to think strategically (Rosenbloom 2002).

Should contain experts with good knowledge of the nationalculturesince the current market structure is globally inclined (Rosenbloom 2002).

The institution in question should ensure that there is the inclusion of representatives from various parts of the world in the CDD team. These can help in the identification of data sources and as such help in the verification of the authenticity of various identities (Rosenbloom 2002).

The CDD team should comprise of a group of experts in the law with a good knowledge of law in various parts of the world

According to Steiner & Marini (2008, p. 14), the objective of CDD should enable the AML of a financial institution to predict with confidence the type of transactions that a customer is likely to hold. This cannot be achieved without tight and secure quality controls in place.

Conceptually, CDD procedures begin by verifying the identity of the customer along with an assessment of the risks that may be associated with that particular customer. Enhanced CDD for high risk customers is highly recommended together with continuous due diligence of the customer base (Financial Action Task Force 2006).

An effective CDD system should comprise of effective policies, processes and procedures to ensure compliance of the financial institution with the regulatory requirements that would allow the institution to report any activity deemed suspicious (Steiner & Marini 2008, p. 14). Furthermore, a robust system of CDD should be implemented with effective protection mechanisms equally directed to both the institution and its customers, considering, Data Protection Act provisions as well as the privacy rights of the customer. An effective CDD system should be cost effective and as such, it should deliver benefits to the institutions while respecting banking practices in the case of a banking institution (Mills 2011)

It is important to bring out the point that CDD systems are meant to protect banks and other financial institutions from reputational, operational, legal and application risks among others, as these would result in large financial costs (Booth et al. 2011, p. 218). They are also made to ensure that financial institutions have sufficient knowledge of their clients and as such, this is meant to ensure that banks and other financial institutions do not accept customers who are outside their normalized risk tolerance or in other words, clients engaging in any unlawful business.

Knowledge of a client’s involvement in money laundering or terrorist financing is important as banks and other financial institutions, who fail to understand their clients, put themselves at risk of significant financial loss. Therefore, effective CDD systems should make it difficult for clients to disguise ownership of accounts within banks. As such, adoption of procedures such as ‘ know-your-customer’, should be adopted within individual jurisdictions, as this forms part of effective CDD programs or systems (Booth et al. 2011)..

An effective CDD system seeks to ensure clear statements of the general expectations and specific responsibilities of staff. Thus, the management should allocate duties clearly with regards to who is responsible for reviewing or approving any changes to established risk ratings or to the profile of customers. As such, the AML of financial institutions should ensure sufficient customer information, since this is significant for the implementation of an effective system for monitoring suspicious activities (Schott, World Bank & International Monetary Fund 2006).

Insufficient customer information may make it hard for an AML to detect money laundering therefore, CDD system effectiveness can be achieved by incorporation of guidelines for the resolution of issues should the information obtained be inaccurate or insufficient (Mills 2011). In addition, current customer information maintenance is important if a CDD system is to be termed as effective.

Notably, CDD should begin by identifying the customer along with the verification of their identity by use of independent source documents,

information and data. At the same time, AML should ensure that the provisions of the Data Protection Act are complied with (Hopton, 2009 p. 42). The due diligence process should be carried out on a risk sensitive basis (Steiner & Marini, 2008). Besides, the measures taken should ensure consistency with the competent authorities along with enhanced due diligence applied to higher risk categories of customers. Simplified measures should be applied to lower risk customers. Strict compliance with the legislative laws should be observed (Booth et al. 2011). Accordingly, a high degree of transparency should be applied in the various transactions and as such, CDD should be applied in the preliminary stages of the establishment of a business relationship or in cases of excess cash transaction preparation (SchottWorld Bank & International Monetary Fund 2006, p. 44).

Discussion of the risks, should there be gaps in the CDD processes

Following the globalization of businesses, global financial systems operate with clients from all over the world. In this context, it is important to note that if CDD measures are not appropriately applied, then, this gives an opportunity for various losses. As such, failure to conduct CDD can lead to a reputational risk which translates to adverse publicity as far as the practices of the business are concerned. Inaccurate application of CDD measures may in this case lead to a loss of public confidence and as a result, may jeopardise the integrity of the institution. Subsequently, borrowers, investors, depositors and other stakeholders may cease business with that institution should scandals arise (Booth et al. 2011).

Apart from the reputational risk, failure to conduct a careful CDD may lead to an operational risk. An operational risk refers to the loss incurred as a result of failed or inadequate processes, systems, external events and people involved. In addition, there is also a legal risk when one fails to carry out a full CDD measures (i. e. when one happens to leave gaps in the required processes). In particular, a legal risk has to do with the potential for law suits once involved in a money laundering case. Again, it may result in sanctions, unenforceable contracts, penalties and fines which may translate to significant financial costs (Steiner & Marini 2008). Furthermore, the institution's licences may be revoked and this may lead to the closure of the institution and as such, may be expensive for the institution since the losses involved may be costly (Fagan & Munck 2009).

Likewise, there is also the risk of concentration associated with the losses emerging from excess credit or loan disclosure to one borrower. Therefore, a lack of knowledge of the customer and the customer relations with the other borrowers may place a bank and any other financial institution at risk (Marks et al. 2012). This may also be a concern when there are related counter-parties, common income sources, connected buyers or assets for repayment. A robust CDD will need to apply KYC (Know Your Customer) which entails the identification of the customer through their national identification card, location, address and other related documents (Demetis 2010, p. 64). This should be incorporated together with the KYCB (Know Your Customer's Business) and as such, this is achieved by means of transaction profile, nature and type of business along with the sources of funds (Knight, International Monetary Fund & Monetary and Exchange Affairs Dept 1998).

Furthermore, the CDD should further apply KYT (Know Your Customer's Transactions) which enables the management to know the customer's transactions through a continuous and careful monitoring of transactions. In addition, a CDD system will work well through the application of KYE (Know Your Employees) which is meant to examine the institution's employees by carrying out background checks along with a continuous monitoring of the systems for trustworthiness andloyaltyto the institution (Alldridge 2003). Moreover, there should be continuous monitoring of customers in order to establish whether there are customer behaviour changes over time and in this case, transactions and other related activities should be monitored (Demetis 2010).

It is imperative to note that a professionals within the financial sector can be sued for failing to perform due diligence. This is due to the fact that the institution has the obligation to conduct CDD and thus should be able to prove to any third party that every effort was made to ensure CDD (Tabb 2004) Similarly, if CDD were to fail, in such a case it would be advisable for the AML to close the account of that particular customer and as such to decline establishing a business relationship while ensuring that a suspicious transaction report is made.

Money Laundering and the Law

The approach of the FATF in recommending that the implementation of CDD measures

should be set out in law is viable and realistic in terms of the practical application of such legislative changes. This is due to the fact that setting

the CDD measures in law will ensure that legal action can be taken to deal with cases where the CDD measures have not been applied appropriately. Again, setting CDD measures out in law will improve the effectiveness of CDD measures carried out on various customers. Taking the example of the first CDD measure recommended to be set out in law, will ensure that the names of the customers are known, the location, country of origin, web data sources verified and as such customer contacts taken into consideration (Demetis 2010, p. 64).

In thisrespect, it will be mandatory for financial institutions to ensure that they only deal with customers with whom they are familiar. As a result, this will translate into effectiveness in the control of money laundering. In fact, this will ensure that all customers provide their details since it would be a requirement of the law along with the fact that this will also be incorporated in institutional policies and procedures. Therefore, before signing into any business relationship, customers and the institution in question will be governed by law, and failure to comply with this will lead both the customer and the institution in question to be held responsible.

In reference to the second CDD measure to be set out in law, it is vital and realistic in the sense that the beneficial owner identity information will be disclosed, and any failure to comply would call for legal action to be taken against the customer. In this sense, it will not be difficult for banking and other financial institutions to get such information as it will be set out in law. Again, the institutions will avoid conflicting with the law as they will have to comply with the CDD measures.

As far as the third CDD measure recommended by the FATF to be set in law is concerned, it is worth noting that obtaining information concerning the purpose and the intended nature of the relationship of the business will be a requirement of the law. As such, it will be required by the customer to avail such information as a requirement of the law rather than of the bank. This will make the work of the banking institutions and other related institutions much easier. Furthermore, the institutions will be forced to comply with the requirement of the law to implement the CDD measures.

On the other hand, the fourth CDD measure recommended by FATF to be set out in law requires conducting a continuous monitoring of CDD on the relationship of the business while scrutinizing the transactions undertaken in the course of the relationship. Such monitoring ensures consistency in terms of the business and risk profile together with the source of funds. Once these are set out in law, it may be vital but not realistic in the practical applications in the sense that the privacy of the customers along with the institutional processes may be compromised (Evanoff, 2009).

Subsequent to setting the financial principle that financial institutions should conduct, CDD should be set out in law with an aim that this will force institutions to comply; otherwise legal action would be taken. Again, such a step would translate to high levels of compliance by the institutions in question and as a consequence, effectiveness of anti-money laundering will be realized.

NPMs and the Law

The FATF recommendations requiring financial institutions to conduct CDD are viable and realistic, except for the fact that new payment methods (NPM) mean the law may need to more fully consider newtechnology. Notably, with an institution intending to make use of NPMs, money laundering may be inevitable. NPMs are well known for their vulnerability to money laundering and terrorist financing. Use of ATMs, prepaid cards, mobile and internet banking has presented a great opportunity for money launderers. However, there are some countermeasures that can prove viable. For instance, one countermeasure may be the implementation of a robust identification and verification procedures (FATF Report 2010).

Such countermeasures may place limits on the transaction amounts and frequency, and include strict systems of monitoring of these aspects. In fact, not all NPMs are subject to law in all authority and as such, they take in the use of internet and mobile payment. Most NPM providers offer their products or services through both internet and mobile interfaces (i. e. virtual) and the FATF recommendations do not specify the specific risks involved and as such, NPM providers may not apply the CDD measures (FATF Report 2010). In this case, the practical application of such legislative changes as recently recommended by FAFT may not yield fruits especially with the use of NPMs. In spite of the challenges associated with the use of NPMs, it is important to note that the electronic records produced in this case can help with law enforcement (Marks et al. 2012).

Importantly, a firm seeking to provide NPM as part of their service should consider the fact that there are three typologies depending on which one chooses to use. Here, the typology has to do with the third party funding whereby cards can be funded through the bank, cash and person to person transfers (FATF Report 2010, p. 36). In addition, there is a second typology which includes the exploitation of a virtual nature (face-to-face) of NPM accounts (FATF Report 2010, p. 40). This typology has the highest potential to facilitate criminals in money laundering. On the other hand, if the firm chooses the third typology (complicit NPM providers or their employees) there is also a high risk, as portrayed in findings made by the IPS where prepaid car providers were controlled by criminals and as such were promoting cases of laundering (FATF Report 2010, p. 33).

From this perspective, where the regulation of NPM service providers are prepared, law enforcement agencies, supervisors, and legislators amongst others, are faced with various challenges. Simplified due diligence, digital currency, and suspicious transaction reporting in cross border cases, and law enforcement against foreign providers with identification of secondary card holders for instance, can go some way to counteract this (Financial Action Task Force 2006),. Therefore, FAFT’s recommendation that financial institutions should conduct CDD, is viable and realistic, except in cases relating to new payment methods (NPM) where its recommendations may have more limited impact.

Conclusion

Following the recent recommendation by FAFT to set the CDD measures out in law, a robust CDD system that would work effectively in this context should contain a team of experts. Specifically, it should contain human resources specialists, functional area managers with cultural understanding of various parts of the world due to globalization,, representatives from various parts of the globe to ensure authenticity of data sources along with a team of information technology experts. This would facilitate the use of New Payment Methods common in the current market and as such, the team of law experts would make this happen in compliance with law in various states of the globe.

References

Alldridge, P 2003 Money Laundering Law: Forfeiture, Confiscation, Civil Recovery, Criminal Laundering and Taxation of the Proceeds of Crime, Hart Publishing, Portland Oregon.

Booth et al. 2011, Money Laundering Law and Regulation: A Practical Guide, Oxford University Press, New York.

Demetis, DS 2010, Technology and Anti-Money Laundering: A Systems Theory and Risk-Based Approach, Edward Elgar Publishing, Massachusetts.

Evanoff, DD 2009, Globalization And Systemic Risk, World Scientific, New Jersey

Fagan, GH & Munck, R 2009, Globalization and Security: Social and cultural aspects. Introduction to volume 2, ABC-CLIO, Carlifornia

FATF Report 2010, Money Laundering Using New Payment Methods, Retrieved on 20th April, 2012 from http://www. fatf-gafi. org/dataoecd/4/56/46705859. pdf.

Financial Action Task Force 2006, Report on new payment methods, Retrieved on 24th April, 2012 from http://www. fatfgafi. org/media/fatf/documents/reports/Report%20on%20New%20Payment %20Methods. pdf.

Hopton, D 2009, Money Laundering: A Concise Guide for All Business, Gower Publishing, Ltd. Burlington.

Knight, MD & International Monetary Fund. Monetary and Exchange Affairs Dept 1998, Developing Countries and the Globalization of Financial Markets, Issues 98-105, International Monetary Fund.

Marks et al. 2012, Middle Market M & a: Handbook for Investment Banking and Business Consulting, John Wiley & Sons, New Jersey

Mills, A 2011, Essential Strategies for Financial Services Compliance, John Wiley & Sons, New Jersey.

Rosenbloom, AH 2002, Due Diligence for Global Deal Making: The Definitive Guide to Cross-Border Mergers and Acquisitions, Joint Ventures, Financings, and Strategic Alliances, John Wiley & Sons, New Jersey.

Schott, PA, World Bank & International Monetary Fund 2006, Reference Guide to Anti-Money Laundering And Combating the Financing of Terrorism, World Bank Publications.

Steiner, H & Marini, SL 2008, Independent Review for Banks – The Complete BSA/AML Audit Workbook, Lulu. com, North Carolina. Tabb, WK 2004 Economic Governance in the Age of Globalization, Columbia University Press, New York.