Financial Exclusion as a Consequence of Counter-Terrorism Financing

Zeynab Malakoutikhah

School of Law

University of Leeds

lwzm@leeds.ac.uk

Purpose: The purpose of this paper is to analyse the unintended consequences, financial exclusion, of counter-terrorism financing regulations in terms of their impact on financial inclusion and consequently the creation of an ineffective counter-terrorism financing framework. A further aim is to make recommendations to mitigate these unintended consequences.

Design/Methodology/Approach: This subject is examined by using the practices of a range of countries and organisations. The interdisciplinary approach of the article is highlighted, which comprises criminal law, banking law, international law, and human rights law.

Findings: Financial exclusion is a focal point which results in ineffective counter-terrorism measures which are caused mostly by the formal financial sector, in particular the banking system. The financial exclusion also leads to counter-productive counter-terrorism financing through a low risk-appetite, de-risking, de-banking, financial exclusion, and using unregulated or less regulated and supervised financial systems.

Originality/Value: No article comprehensively analyses financial exclusion, as a consequence of counter-terrorism financing framework. The paper examines the process of counter-terrorism financing regulations which leads to financial exclusion. In addition, the impact of financial exclusion on all relevant actors, such as individuals, correspondent banking relationships, money and value transfer services, charities, and virtual currencies are examined.

Keywords: Counter-terrorism financing, Financial exclusion, Financial culture, Human rights, Unintended consequences.

Introduction

A rampant demand for countering terrorism finances was launched following the 9/11 attacks. The process of international counter-terrorism financing (CTF) was signalled by the United Nations Security Council (UNSC) Resolutions 1267 (1999) and 1373 (2001), the International Convention for the Suppression of Financing of Terrorism (1999) (‘the Financing Convention’) which came into force in 2002, and the Financial Action Task Force's (FATF) nine special recommendations (2001 and 2004) on combating terrorism financing. CTF at the international and national level consists of three main aspects: the criminalisation of terrorism financing; financial regulations as preventive measures; and sanctions imposed on individuals and entities who support terrorist acts, terrorists and terrorist organisations. The focus of this article is on those regulations which have been imposed on the financial sector, in particular the banking system, as preventive measures for countering terrorism financing. The aim is to analyse the unintended consequences of these regulations in terms of causing financial exclusion and consequently creating an ineffective CTF framework in order to make recommendations to mitigate the unintended consequences.

The effectiveness of setting regulations as preventive measures is mostly based on the risk-based approach which is highlighted as a central issue in the FATF recommendations, and is set out in Recommendation 1. Recommendation 1 includes four main criteria: to identify, assess and understand terrorism financing Risks, to designate an authority or mechanism for coordination, to ensure the adopted measures are commensurate with the identified risks, and to be an essential foundation in allocating anti-money laundering (AML)/CTF resources efficiently (FATF, 2012). Risk is a function of three factors in the form of threat, vulnerability, and consequence (FATF, 2013a). In order to assess the risk of terrorism financing, the following factors must be determined. First, threats are the terrorists, their facilitators, and their funds. Second, vulnerabilities comprise three major sectors, in the form of the formal financial system, the informal financial system, and non-profit organisations, all of which can be exploited by terrorist threats. Third, consequences are the impact and harm which terrorism financing can do to the population, financial sectors, and national and international interests.

The application of the risk-based approach and the subsequent strict regulations within the financial system can be counter-productive and lead to financial exclusion. Financial exclusion can be viewed through two perspectives: the first and most-common perspective, which came to attention in the 1990s, focuses on the level of financial capability of customers, their level of knowledge and their ability to make financial decisions (Blake and De Jong, 2008), which can lead to poverty and social exclusion (Koku, 2009; Solo, 2008; World Bank, 2008). The second perspective which is the core element of this paper, is the financial exclusion caused by the conflict between the liberalisation of the financial industry through deregulation (Koku, 2015) and strict regulations imposed on the financial system, such as counter-terrorism financing regulations, which hinder access to financial services. The deregulation of the financial industry seems to have led to difficulty because financial institutions are encouraged to boost shareholders' profit (Koku, 2015), rather than paying attention to vulnerable customers or the needs of society. The result of financial exclusion in terms of the second perspective leads not only to social injustice, but also to an ineffective CTF framework.

The revised FATF Guidance on Financial Inclusion (2013), declared the issue of financial inclusion and encourages financial institutions to use a flexible risk-based approach, with the purpose of increasing financial inclusion while countering terrorism financing (FATF, 2013b). However, this issue remained as a concern and led to the 2017 CTF framework in which the FATF Customer Due Diligence Supplement expands on the previous guidance (2013) with a special focus on the making progress on financial inclusion. This is done through several recommendations, including increased financial education, expanded access to regulated financial services for low-income and under-served people, and more reliable proof-of-identity systems provided by governments (FATF, 2017). However, the practice of financial exclusion as a result of the CTF regulation remains unsolved, as illustrated in this paper.

Financial exclusion undermines the legitimacy and the effectiveness of CTF regulations, and the procedure which leads to financial exclusion is not a fair procedure. Regarding legitimacy, financial exclusion violates human rights. Financial inclusion is associated with other human rights such as economic growth, development, job creation, and eliminating poverty (FCA, 2016). In terms of effectiveness, access to financial services not only precludes progress in terms of the implementation of CTF, but also helps to identify and prevent financial crimes such as terrorism financing, by bringing people under the umbrella of effective regulation and supervision. The more access to a regulated and supervised financial system, the less financial exclusion there will be, and subsequently the more effective the CTF framework will be. Encouraging unregulated or less regulated and supervised financial sectors instead of a formal financial system will have an adverse impact on the CTF framework. Financial exclusion derives from different kinds of exclusion, including access exclusion, condition exclusion, price exclusion, market exclusion, and self-exclusion. The only exclusion relevant to the aim of this paper is access exclusion, which is the restriction of access as a result of the process of risk assessment (Carbo *et al*, 2007). Thus, to assess the legitimacy and effectiveness of the CTF regime, this article makes an attempt to examine how CTF might lead to an ineffective CTF regime through financial exclusion, and what can be done to ensure financial inclusion while still countering terrorism financing.

This article's contribution to the discussion of the CTF is examining the unintended consequences of the CTF framework, in particular the preventive measures applied to the banking system. To this end, this article is divided into three sections. First, the external exclusionary effects, which stem from the CTF regulations as preventive measures applied to the banking system, are discussed in order to reveal that to what extent the preventive measures are required and are necessary. The second section pertains to demonstrate the internal exclusionary effects which are derived from financial culture. This process includes a consideration of risk-appetite, de-risking, de-banking, financial exclusion, using an unregulated or less regulated and supervised financial system, and an ineffective CTF framework. The third section elaborates on the practical impact of the CTF regulations and the financial culture on individuals, correspondent banking relationships (CBRs), money and value transfer services (MVTS), especially the *hawala* network, charities, and virtual currencies (VCs).

External Exclusionary: Counter-Terrorism Financing Regulation

The CTF preventive measures must be applied to formal financial institutions, in particular the banking system as one of sectors at the risk of terrorism financing. These preventive measures are explained in detail by the FATF Recommendations (FATF, 2012), but also are mentioned in other instruments such as the UNSC Resolutions, relevant Conventions, World Bank, International Monetary Fund (IMF), and Egmont documents. The UNSC Resolution 1373 declared that 'all states shall prevent and suppress the financing of terrorist act'. The Financing Convention (1999) requires states and financial institutions to 'utilise the most effective measures available for the identification of their usual or occasional customers, as well as customers in whose interest accounts are opened and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity', 'adopting regulations prohibiting the opening of accounts the holders or beneficiaries of which are unidentified or unidentifiable', and regarding the identification of legal entities 'to take measures to verify the legal existence and the structure of the customer by obtaining, either from a public register or from the customer or both, proof of incorporation, including information concerning the customer name, legal form, address'.

However, the UNSCRs, the Financing Convention and other guidelines released by different organisations, such as the FATF and the Joint Money Laundering Steering Group (JMLSG) are not complete and comprehensive and fall short in providing any detailed methods, because their focus is generally on the criminalisation of terrorism financing, as a first aspect of CTF framework. The methods of preventive measures are left to each country and financial institution's decisions. Based on the FATF recommendations and above-mentioned instruments, the preventive measures in financial institutions can be undertaken through three leading mechanisms: customer due diligence (CDD), monitoring system, and suspicious transaction reports (STRs) which are explained below.

Customer Due Diligence

One of the main impediments against financial inclusion is the lack of acceptable identity documentation and data verification by banks (FATF, 2017). The first and foremost preventive step for banks is to prohibit the opening of accounts for unidentified or unidentifiable holders or beneficiaries. To this end, the leading method is to Know Your Customer (KYC) through having effective customer due diligence (CDD) system in place. The CDD should involve identification and verification both customer's identity and the beneficial owner; understanding and obtaining information on the purpose and nature of the business relationship; and conducting ongoing due diligence on the business relationship (FATF, 2012). The KYC mechanism refers to banks and other financial system monitoring and auditing information about their customers and beneficial owners before engaging in financial business with them (Biali, 2012). The KYC approach assists banks to recognise their customers: who they are, what their jobs are, and why they require banking services. Effective KYC has two stages: obtaining and verifying identification.

The KYC, in practice, has some difficulties. The first one is related to the first stage - obtaining identification. The legal name, payment address, telephone number, date and place of birth, nationality, and occupation must be obtained. The second issue is in relation to the verification of the obtained ID. Based on the Basel Committee's guidelines, verification can involve the following methods: confirming the date of birth from an official document; confirming the permanent address through several ways such as the provision of a utility bill; contacting the customer to ensure the details provided are correct; and confirming the valid ID through an authorised person such as an embassy (Basel, 2003). These stages often cannot be easily carried out for several reasons. For example, a citizen's name may not exist on a comprehensive national identity base; and their birth may not have been registered and/or they may not have reliable documents that can verify their identity both in developed and developing countries (Koker, 2011). This may lead to financial exclusion, which is contrary to the effective AML/CTF framework because providing financial inclusion depends on the accurate identification of citizens (ITU, 2016). The ITU Research on 48 national identity programmes in 43 developing countries[1] reveals that only half of the programmes have connection between National ID and financial sectors (ITU, 2016). In accordance with the survey undertaken by the World Bank Group in 2017, among who do not have a bank account, 20% responded lack of necessary documentation as one of the reasons, among other reasons such as no enough money (66%), too expensive (26%), family member already has account (26%), distance (22%), lack of trust (16%) and religious reasons (6%) (The Global Findex Database, 2017). By analysing the mutual evaluation submitted to the FATF by twenty developed countries, thirteen countries[2] were rated as being largely compliant, six countries[3] as being partially compliant and two countries[4] as being non-compliant in terms of CDD (R.10) of the FATF. This means that even by applying CDD based on the risk-based approach, which is one of the reasons for financial exclusion, these countries will have to apply stricter regulations in order to be rated as being compliant.

Monitoring System

At the second stage, after KYC, banks should create a risk profile for each customer based on the individual customer's risk level or homogenous characteristics. Based on the risk level of each customer, banks can adopt enhanced due diligence (EDD) or simplified due diligence (SDD). EDD is conducted when the customer or product and service rendered is regarded as a high-risk, such as in the case of transactions linked to higher-risk countries, unnecessarily complex or beneficial ownership structuring, unusual or lacking an obvious economic purpose (FCA, 2018). In contrast to EDD, if the lower risk is identified based on CTF/AML assessment of each country, it is allowed to undertake SDD (FATF, 2012). Conducting ongoing due diligence with regard to the business relationship and transactions can be an effective tool to ensure that such transactions are consistent with the knowledge obtained about the customer's identity card, risk profile and the nature of the customer's business (FATF, 2012). Without ongoing monitoring, banks are likely to fail to identify and report suspicious transactions. The rationales behind monitoring are to make it difficult for terrorists use financial systems and to provide information to law enforcement (Joint Money Laundering Steering Group, 2017). Generally, the system of monitoring can be based on the level of sensitivity of each risk profile; those with a high-risk profiles, such as politically exposed persons (PEPs) (Edmond, 2017; FATF, 2013c), when a person provides false identification, a transaction is complex and unusually large, or a transaction has no economic or legal purpose, must be subject to EDD monitoring system (Joint Money Laundering Steering Group, 2017). Further, EDD must be applied relating to the position of a jurisdiction, its reputation and standing in terms of ML/TF risks. As an example, based on the European Commission Regulation 2016/1675, 11 countries,[5] including Afghanistan, Iran, Iraq, and Syria are considered as high-risk third countries[6] based on several factors, including geographical factors, membership of groups that admit certain required benchmark, contextual factor, evidence of relevant criticism, mutual evaluation reports, implementation standards, and incidence of trade with the jurisdiction (Joint Money Laundering Steering Group, 2017).

However, EDD should not lead to financial exclusion and consequently violate human rights. Financial institutions should not refuse to open accounts or business relationships that are only based on the customer being high risk. Only in the situation where a sector cannot satisfy itself as to the identity, verify the identity, or obtain sufficient information, should it not enter into, or terminate a business relationship (Joint Money Laundering Steering Group, 2017). In reality, due to sanctions on banks that fail to apply and monitor situations using the risk-based approach, the banks tend not to enter into a business relationship with high-risk customers (Goodway, 2014). For instance, some UK banks refuse to open or they even close the accounts for Iranians or Syrians living in the UK; and some have not explained the reasons for these actions while others cite the sanctions against these countries as a main reason (Kamali Dehghan, 2017). The closure of the accounts is only based on the advanced notice from the banks without any mentioned reasons since 'banks are entitled to choose its customers' (*Dahabshiil v. Barclays)*. It seems that because of fear from being penalised, banks decline customers with high risk. Consequently, the overcompliance by banks can be regarded as an unfair action. Cases have arisen involving Iranians in the UK who have sued banks over racial discrimination because the banks had refused to open an account based on the passport of the customers, while the banks, such as RBS, claim that the closure of the accounts was not because of the race or religion (Kamali Dehghan, 2017), but the banks did not explain the reasons for their actions.

Suspicious Transaction Reports

Another core element of preventive measures associated with the financial system is the requirement that financial institutions must report suspicious transactions to the competent authorities. Financial information is a powerful tool in the investigation and gathering intelligence (HM Treasury, 2007). The FATF hypothesis is that Suspicious Transaction Reports (STRs) will generate quantitative and qualitative law enforcement outcomes (Chaikin, 2009). The prominence of STRs is emphasised by the Financing Convention (1999) which states that it is the obligation of the financial institutions to report all complex, unusual large transactions and unusual patterns of transactions which have no apparent economic or lawful purpose. Although the Financing Convention clarifies some kinds of transactions to be reported, these elements, such as complex or unusual large transactions, are not clear or precise. In this regard, the FATF (2012) only refers that if financial institutions 'suspect or has reasonable grounds to suspect', they must report the suspicious transactions to the competent authorities. The FATF recommendations also do not clarify what constitutes suspicion and what reasonable grounds for such a suspicion may be.

Because of the fear of violating regulations, the number of STRs has markedly increased over the years. In the UK, the number of Suspicious Activity Reports (SARs) was about 200,000 in 2006, compared to 400,000 in 2016/17. More that 70 percent of all STRs submission for terrorism financing is from the banking sector from 2015 to 2018 (UK National Crime Agency, 2017 and 2018). The numbers of SARs submitted for terrorism financing in the UK were 1,414 (October 2015 to September 2016) and 2,688 (April 2017 to March 2018) (UK National Crime Agency, 2017 and 2018). This demonstrates that the rigid responsibilities placed on banks lead to the generation of STRs, which are submitted based on 'suspicious' or 'reasonable' grounds, and it is difficult to understand the effectiveness of these STRs. At EU level only 10%, and in the UK only 5-7% of STRs lead to further investigation (Law Commission, 2018).

There are several explanations for high number of SARs which are not effective for law enforcement (Law Commission, 2018) and might lead to indirect financial exclusion and an ineffective CTF regime. First, a low threshold for criminality is applied; most countries, such as the UK, adopt an 'all-crimes' approach as predicate money laundering offense. The reporters are not obliged to identify a specific terrorism offense which the monies are linked to (Law Commission, 2018). In accordance with the UK's statistic, the number of SARs for terrorism financing is far less fewer than for money laundering, which shows that when they suspect the monies are the proceeds of a crime, they will submit SARs for money laundering not for terrorism financing because the reporters are not able to say whether the predicate crime is terrorism financing (Law Commission, 2018). After the terrorist attacks in London (2017) (BBC, 2017), some banks in the UK submitted SARs to close some accounts which had transactional relations with one of the attackers or even had lived in the same street (Law Commission, 2018). This trend illustrates that not all SARs are issued on reasonable grounds. Second, individual criminal liability; individuals in the regulated sectors are at risk of criminal liability for failure to report due to negligence. As a result of this, individuals prefer to submit unnecessary STRs rather than taking the risk of prosecution for a failure to report. Third, strict regulations apply to hinder any flexibility or judgement to be applied. So, the strict regulations create confusion and misunderstanding and consequently lead to the unnecessary STRs.

Fourth, the meaning of suspicion is very broad, ill-defined and unclear. No definition for the term 'suspicion' has been released, even by the FATF. The STRs are based on the individual perspective of the employee conducting the transactions (Lafolla, 2018). This uncertainty will lead to two dilemmas; it either increases the risk of individual criminal liability if they do not submit STRs, or it causes the high number of submitted STRs. Thus, both wide definition of terrorism offences and low threshold for reporting cause 'defensive reporting' which more STRs are because of concern concerning a failure to comply CTF regulations (Law Commission, 2018).

As a result of imposing the obligation on banks to report suspicious transactions, they have obtained more authority and discretion concerning suspicious transactions. As mentioned before, the regulator leaves this issue to financial institutions to determine what the suspicious transactions are and how to comply with the regulations (De Goede, 2018). The more regulatory burden the financial institutions have, the more suspicious transactions they report, because of the fear of regulatory consequences.

The submission of STRs has indirect effects on financial inclusion. As mentioned above, the STRs is mostly submitted for four reasons: a low threshold of criminality, individual criminal liability, strict regulations, and the broad concept of suspicion. Due to the imposed fines and penalties, and the requirement for banks to invest in experienced staff, control-related training, and sophisticated technology, banks tend to not deal with some categories of customers such as high-risk customers, in order to mitigate the risk of reputation damage, being penalised and enduring extra expenditure. Therefore, these elements cause some customers to be ultimately excluded from financial services.

Internal Exclusionary: Financial Culture

The process of internal exclusionary which leads to ineffective counter-terrorism financing has six stages: risk-appetite, de-risking, de-banking, financial exclusion, using unregulated or less regulated and supervised financial systems, and ineffective counter-terrorism financing, which are explained below with particular focus on stage four, financial exclusion.

The first stage relates to low risk-appetite. Risk-appetite can be defined as '…the amount of risk that an organisation is prepared to accept, tolerate, or to be exposed to at any point in time' (HM Treasury, 2006). As the risk must be well-recognised and well-managed, banks need to spend more money on investing in experienced staff, control-related training, and sophisticated technology. Regarding the cost of the implementation of risk-based approach, several banks have declared the extra expenditure required for the implementation of risk-based approach. For instance, HSBC suggests $750-800 million, and the Australian investment bank Macquarie, $320 million (Keatinge, 2014a). The expenditure, reputational risk, and strict counter-terrorism financing regulations result in low risk-appetite on the part of banks.

The second stage is de-risking; 'De-risking refers to the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF's risk-based approach' (FATF, 2014a). As de-risking is not based on a case-by-case assessment, and it terminates the relationship with entire regions, customers and countries, it raises difficulties and dilemmas in terms of the implementation of the CTF framework. The relevant leading drivers for de-risking are the high cost of compliance with the CTF/AML regime based on risk-based approach, the high level of financial penalties, and the cost of the implementation of the sanctions regime (FATF, 2016).

Figure 1: The Process of Counter-Productive Regulations

The third stage is de-banking; the practical element of the policy of de-risking can be observed as not rendering basic banking services, such as not opening an account or even closing the existing accounts of high-risk customers. It is estimated that approximately 1.7 billion unbanked people have no access to safe and reliable financial services, mostly in countries in Africa and South-East Asia which are affected by terrorism (UN, 2019).

The fourth stage is financial exclusion; the generation of financial exclusion, including limited access to formal financial systems, has been a criticism of the AML/CTF regime (Shehu, 2012). There are potential barriers to the formal financial sectors which arise from geography, cost, cultural mistrust, lack of understanding of financial services, language, and lack of identification documents (Koker, 2011). Those who do not have access to financial services are usually socially and financially vulnerable (Koker, 2006). Financial exclusion impedes social and economic development (Koker, 2006). 73% of the excluded people live in only 25 countries.[7] By analysing the FATF mutual evaluation report of these countries, it can be concluded that more than half of these countries are not able to comply with FATF

Recommendation 10 (CDD). Of these 25 countries, ten[8] were rated as non-compliant, eight[9] as partially compliant and seven[10] as largely compliant. The efforts should go toward financial inclusion which means '…providing access to an adequate range of safe, convenient and affordable financial services to disadvantaged and other vulnerable groups, including low-income, rural, immigrants and undocumented persons' (FATF, 2013b). Financial inclusion is an enabler for other Sustainable Development Goals (2015-2030), including eradicating poverty, ending hunger, and promoting economic growth.

The fifth stage is the phenomenon of the increased use of unregulated or less regulated or supervised financial systems, such as money and value transfer services (MVTS) such as *hawala, hundi, fei-chien,* and the *black market peso exchange* (FATF, 2012). The increased use of MVTS is because the specific category of customer are excluded from access to banking services. Prior to 9/11, MVTS were largely unregulated around the world (FATF, 2005). The FATF statement in 2017 stated that 'without access to the formal financial system, unserved or underserved customers will resort to cash and unregulated channels, which limits transparency and increases the risk of crime…'. After the 9/11 attacks, international organisations and countries demanded increased control over MVTS. However, MVTS is not under control and monitoring in the same way as the banking system, as it is not a formal financial system.

The result of this process is reflected in the sixth stage which is the ineffective counter-terrorism financing regulations. The goal of the CTF regime is to attract people and institutions to the financial system, because it is highly regulated and supervised, while the low risk-appetite results in the tendency of people and institutions to use unregulated or less regulated and supervised financial systems. This is against the purpose of counter-terrorism financing. This issue in practice is examined in detail in the next section.

The Impact of Financial Exclusion

Individuals

The first form of financial exclusion only targets individuals and does not have systematic effects on any jurisdictions or special entities. The percentage of unbanked adults in developing countries is 72%, while in developed countries is 19% (FATF, 2013b). As the goals of financial inclusion and the CTF regime are complementary, this means that an effective CTF regime should promote or at least not disincentives' financial inclusion. The main policy should be to attract people into the formal financial system, since this is the goal of financial inclusion. On the other hand, financial exclusion has a direct linkage to the less effective CTF regime, because the amount of large informal, unregulated and undocumented institutions can affect the whole financial services (FATF, 2013b).

The key question here is how to create a balance between the implementation of the CTF regime and financial inclusion. There is evidence that the main problem when it comes to attracting customers to a formal financial system is the robust CDD requirements, especially the identification and verification of a client's identity (Shehu, 2012). Although the FATF has identified recommendations and policies for countries in order to prevent TF and ML, based on the different conditions of each county, these recommendations can be tailored to maintain their flexibility and effectiveness. Nevertheless, the strict FATF recommendations may open up the possibility of corruption or evasion, such as by using informal financial institutions which are less regulated and less supervised. There is a limit to the 'one size fits all' solution, in that 'what works in one jurisdiction may not necessarily work in another' (Shehu, 2012). In fact, there is a negative correlation between financial exclusion and using informal financial system. Without sufficient measures in terms of financial inclusion, the robust CTF regime and FATF recommendations only apply to the formal financial system, while many more people are driven to use informal financial systems.

There is a wide array of possible solutions to maintaining a balance between the CTF regime and financial inclusion. First, there is 'tiered CDD' by which clients have access to a range of services based on the extent of the identification/verification provided. Second, there is the restriction in terms of product functionalities, such as face-to-face dealing or limitations in terms of geographical transactions. Third, the list of valid documents for identification purposes can be widened (FATF, 2017). However, the simplified CDD must be based on the law, because the formal financial systems, in particular banks, are reluctant to take risks. In different situations, banks face significant fines and risks to their reputations due to inappropriate risk rating. In 2012, HSBC (UK) was fined more than US $1.9 billion for facilitating the transfer of millions of dollars resulting from Mexican drug trafficking organisations (Stanley and Buckley, 2016). In 2014, Arab Bank was convicted for supporting Hamas and direct facilitation of 24 terrorist attacks; in 2015, BNP paid $140 million fine for violating sanctions against Sudan, Cuba, and Iran (Ramachandran, 2015).

Correspondent Banking Relationships

The second action which leads to financial exclusion is the withdrawal of correspondent banking relationships (CBRs). The CBRs involve one bank (the correspondent) providing a deposit account or other liability accounts, and related services, to another bank (the respondent), often including its affiliates (IMF, 2016). The CBRs facilitate a range of transactions and services. In some countries, without CBRs, they encounter financial exclusion as CBRs are a lifeline to the economics of these countries (Magazine, 2017), although in accordance with the risk-based approach, a financial firm can terminate its relationship with specific correspondents. In recent years, there is a sharp decline in the number of CBRs which raises a specific concern (FSB, 2017). Globally, 75% of 20 large international banks reported a decline in CBRs from 2012 to mid-2015 (World Bank, 2015a).

The decline in CBRs has led to the undermining of the process of financial inclusion. Due to compliance with the CTF/AML framework, some countries have closed their accounts with the Central Banks. Countries in the Middle East which are affected by terrorism and international sanctions are most affected by the withdrawal of CBRs (IMF, 2016). The withdrawal of CBRs is based on the cost-benefit analysis which has a direct association with compliance with the CTF/AML framework, fear of fines and penalties, and reputational risks. However, two main reasons for withdrawal of CBRs by large international banks, which act as correspondent for thousands of other banks, are about concern on ML/TF risk and imposition of international sanctions on a jurisdiction (IMF, 2016). Regarding the regulations, the lack of clarity on the scope of CDD and more expenditure for submitting STRs may result in terminating CBRs. For instance, a survey on large penalties for CDD in the US are related to sanctions, AML/CTF, and tax respectively (IMF, 2016). The uncertainty regarding CDD engenders imposing strict regulations by the banks in order to prevent fines and penalties.

The cross-border CBRs are considered 'inherently' high risk by the FATF which means not only the simplified CDD measures are never appropriate, but also additional CDD must be applied in this context. As a result, recommendations 10 (CDD) and 13 (CBRs) must be met in all cases of cross-border CBRs. Recommendation 10 (CDD) was explained, but in terms of recommendation 13 there are some arguments. One reason which makes problem is Know Your Customer's Customer (KYCC) which is not necessary under the FATF Recommendations. The only responsibility for CBRs to prevent terrorism financing is to monitor respondent's institution transaction and business, and to assess the respondent institution's AML/CTF controls (FATF, 2016). The CTF control can comprise reviewing the independent audit and a third party, interview of compliance officer, and potentially on-site visit (FATF, 2016).

Money or Value Transfer Systems

Due to the increased surveillance associated with formal financial sectors, terrorists may use Money or Value Transfer Systems (MVTS) (Passas, 1999),[11] which are less supervised and less regulated. An MVTS is defined as "…a financial service that accepts cash, cheques, other monetary instruments or other stores of value in one location and pays a corresponding sum in cash or another form to a beneficiary in another location" (FATF, 2012). The suspicions with regard to MVTS, such as *hawala, hundi, fei-chien,* and the *black market peso exchange* (FATF, 2012), originated from the early 1990s, because of their vulnerability to money laundering, drug trafficking, and misuse by the migrant diaspora community (Cooper and Walker, 2016).

In this section, the focus is on the *hawala* system as one of the most popular MVTS in South Asia, the Middle East, and even in European countries (Sambei *et al*, 2009). *Hawala* means 'to transform', or 'to change' (De Goede, 2003), and has been used in several countries for centuries. The reaction to the *hawala* system after the 9/11 attacks has been severe. For instance, President Bush stated that "…by shutting these networks down, we disrupt the murderous work" (De Goede, 2003). While the survey illustrates that the main reason to use *hawala* is not criminal advantage even though *hawala* is regarded as a sector at risk to ML/TF (FATF, 2013d). Although the international concentration on the *hawala* system is necessary based on the risk-based approach, this system is very often the core method for legitimate purposes in different areas.

Remittances contribute to maintaining the welfare of approximately 700 million people, and developing countries receive over $400 billion in remittances annually (Keatinge, 2014b), which represent the main income source for food, healthcare, housing, and education (World Bank, 2015b). Regarding the humanitarian situation, *hawala* is the cheapest and most efficient method of transferring money, as in the case of the 2011 famine in Somalia, the UNICEF declared that ‘the use of *hawala* was extremely efficient’ (UNICEF, 2013). As an example, between 80% and 90% of financial transfers in Afghanistan involve *hawala* transactions (Trausolt and Johnson, 2012). NGOs alone transfer at least $200 million in emergency aid, humanitarian relief, and development financing to Afghanistan through the *hawala* system (Razavy, 2005).

Financial exclusion through limiting services of the MVTS engenders the poverty and less economic growth. As mentioned before, the withdrawal from the business relationship is based on the cost-benefit analysis. For banks, serving MVTS does not have immense benefits considering the risk (Nicoli, 2018). The justification for most banks is that complying with CTF regulations is no longer commercially worthwhile to provide MVTS, which have less than £100,000 in annual revenue (Ramachandran, 2015). The unfairness leads to existing small business out of the market and eliminating competitions in this business. The allegations of the US against *Al-Barakat* remittance operator for supporting the Al-Qaeda network leading to shutting it down, led to a crisis in Somalia (*Dahabshiil v. Barclays*), where the families of immigrants could not receive money (50% of Somalis depend entirely on these funds) (De Goede, 2003). It also affected labour, and investment opportunities, and the construction and transportation systems (Razavy, 2005).

There are several *hawala* networks that had their accounts closed when banks terminated all services provided to them. As an example, in 2013, Barclays Bank closed over 140 UK-based remittance companies due to being high-risk. HSBC terminated its business with remittance companies in some jurisdictions, or Sunrise Community Bank decided to close all accounts of US-Somali remittance in order to be compliance with the CTF regime (Ramachandran, 2015; World Bank, 2015b).

However, a survey completed by 25 banks and 82 MVTS in the G20 countries in 2014 demonstrates that the violation of AML/CTF regulations is not the top reason for closure of the MVTS accounts (World Bank, 2015b). The chief reasons comprise profitability, fear of regulatory scrutiny, lack of confidence in the MVTS' procedures, and reputational risk (World Bank, 2015b). Due to the fear governing the relationship between the regulatory authorities and the banking sector, and banks not feeling that they are partners in tracking criminals through the financial system, they will continue to operate conservatively and to restrict services for high-risk customers (Keatinge, 2014b). The remittance companies are regarded as high-risk customers even though they comply with the procedure because the money remitters to the high-risk countries (Ramachandran *et al*, 2018). In this regard, the Dahabshill is an interesting case. As there has been no formal banking system in Somalia since the late 80s, the MVTS plays a leading role in Somalia. The Dahabshill Company has a range of customers, from individuals to international aid charities, such as the UNDP and the WHO (Immigration and Refugee Board of Canada, 2015). On the other hand, the existence of the Al-Shabab terrorist group raises a concern for governments and banks not to benefit Al-Shabab (HM Government and Beechwood International, 2013). In 2013, Barclays decided to close all accounts of the Dahabshill Company and terminate all services, which would cause the negative impacts on food's security, education, and even Somalian business as a whole. The decision on closure was only based on that the remittance system is high-risk without any other justification while the company has a compliance and AML/CTF program on place and Barclays reinforced the satisfactory policies and procedures on the company and had never raised any concern (*Dahabshiil v. Barclays)*. In conclusion, the Dahabshiil Company won the case and obtained a limited injunction to prevent the closure of its accounts pending further decision by the court through the arguments that dominant firm such as Barclays should not be allowed to push its customers out of the market or treat them differently without objective justification (*Dahabshiil v. Barclays*; Fujii-Rajani, 2017).

Subjecting MVTS to de-risking leads to financial exclusion of mostly disadvantaged people, which is not a fair process while combating terrorism financing. Considering a type of customers as inherently high risk without examining case by case and consequently terminating all services is not only fair. Although the MVTS are vulnerable sectors to ML/TF, the aim of CTF framework should be to have safe international remittance services and make effort that the MVTS do not cut off their relationship with the regulated financial system.

Charities

Charities require to access to the banking system for three financial activities and the financial exclusion happens by hampering these financial activities. The first activity is to receive funds or donations; transaction of funds from the high-risk jurisdictions might be delayed, blocked or returned to the donor in the name of CTF policy. The second financial activity is to transfer money; the core aim of the charities is to distribute the collected funds among the targeted community. Sending money for humanitarian aid is one of the challenging issues because of the nature of jurisdictions, such as Palestine, Somalia, Syria and Yemen, to which funds are sent, as some of the jurisdictions are associated with imposed sanctions, the existence of terrorist organisations, corruption, and money laundering. The third activity is to store funds; there are numerous cases that the charities' bank accounts were closed or unable of open bank accounts (Keatinge, 2014a). In the UK, the bank accounts of charities were closed by different banks, such as closing bank accounts of Finsbury Park Mosque by HSBC in 2014, Ummah Welfare Trust by HSBC in 2014 and Barclays in 2008, and Advocacy Group CAGE by the Co-operative Bank (Keating 2014a).

Further, Muslim charities have been considered a risk by many banks and measures continue to be taken daily to hinder them from working effectively (Pantuliano *et al*, 2011). The blockage of Muslim Charities' funds is perceived as a 'Western attack' on Muslims (Gordon and Taraboulsi-McCarthy, 2018). The Islamic Bank of Britain also ended its links with Interpal in 2008 because of pressure from Lloyds TSB, which acted as its clearing bank (Walker, 2014). This process of 'de-risking', not only of listed persons or entities but also of Muslim organisations which operate in conflict zones or have political objectives (including some mosques), is difficult to challenge, but has become increasingly common (Walker 2014; Pantuliano *et al*, 2011). Recently, the British Muslim International NGOs have asserted that they have been 'disproportionately affected' and 'actively discriminated against' by the UK counter-terrorism measures (Metcalfe-Hough et al, 2015). In practice, the access to funding on the part of charities is not equal, and there is a degree of discrimination against Islamic charities, while in accordance with articles 6(b) and (f) of the Declaration on the Elimination of All Forms of Intolerance and of Discrimination Based on Religion or Belief, there would not be any discrimination such as 'to establish and maintain appropriate charitable or humanitarian institutions and to solicit and receive voluntary financial and other contributions from individuals and institutions.' In some cases, only when the Islamic charities changed their name and logo, and ensured that their trustees were known as secular figures, they could open bank accounts (Gordon and Taraboulsi-McCarthy, 2018). As the main pressure is on Islamic charities, this undermines the basic right of Muslims to freedom of association.

In countries under some form of sanctions, such as North Korea, Iran, Myanmar or Syria, aid organisations experience great difficulties when remitting funds to pay local partners. In the case of Syria, for example, OFAC Licence 11 allows payments to be made for humanitarian purposes, and yet the banking sector remains risk-averse and unwilling to accept such licences at face value. Another recent case is related to Iran's devastating flood in 2019, with two million people in need of humanitarian aid. The imposition of US sanctions impeded the humanitarian relief in Iran (Reuters, 2019), as banks would not enter into a business relationship with Iran because of the ambiguity of the regulations, and a fear of fines and penalties for breaching CTF regulations with regard to the sanctioned regimes. It should be mentioned that the International Court of Justice (ICJ) required that the US must remove any impediments arising from the re-imposition of sanctions to the free exportation to Iran of medicines and medical devices; foodstuffs and agricultural commodities; and parts, equipment and associated services necessary for the safety of civil aviation (*Islamic Republic of Iran v. United States of America*). Aid agencies report that banks require extensive evidence to be satisfied that the payments are intended for humanitarian purposes, and even once this is supplied, there is no guarantee that an intermediary bank would not block the funds during transmission. There is also the question of which local banks in such a situation remain operational and liquid (HM Government and Beechwood International, 2013).

Services provided for NGOs are expensive to maintain. Charities are unattractive institutions, such as *hawala* network, for banks because of the combination of risks, fear of fine, and low profitability (Keatinge, 2014a). Banks are cautious in transferring funds to some countries, such as Iraq, Iran, and Syria, even for humanitarian aid (Disaster Emergency Committee, 2019). Banks will tend to sure that how humanitarian agencies will use the funds (Disaster Emergency Committee, 2019). In other words, banks play an extra role of banking and involve in the process of charitable work. Although charities and humanitarian organisations have a desire to be compliant, it is difficult to realise what compliance requires (Gordon and Taraboulsi-McCarthy, 2018) because of ambiguity of regulations and policies adopted by banks. Based on the survey conducted in 2017 by Charity Finance Group,[12] 79 percent of charity respondents have problems in accessing or using the banking system such as transfer delay, accounts closed, and funds frozen (Charity Finance Group, 2018), even without any clear explanation for the reasons (Gordon and Taraboulsi-McCarthy, 2018). As mentioned before, banks as a private sector can choose their clients, however, they are social utilities which are licensed by society to render service to the need to society, not only gain benefits.

The financial exclusion of charities has downsides. First, when the banking system is not available for charities, they use other methods for transfer funds, such as cash couriers, *hawala*, black market, and private bank accounts (Charity Finance Group, 2018). For instance, in 2016, Syed Hoque and Mashoud Miah were convicted of financing terrorism because they used Syria-bound aid convoys to send funds, in cash, to an individual linked to an Al-Qaeda affiliate (Charity Commission, 2017).

Second, charities are shut down which has adverse consequences on civil society. The right to freedom of association is an important right underpinning civil society. The importance of civil society lies in promoting good governance and plays a key role in ensuring transparency, accountability and participation (Howell, 2006). The right to freedom of association has two facets. One is the ability of individuals or legal entities to form or join an association (ICCPR, 1996) while the second is the right to seek, receive and use resources, including human and financial material from domestic or foreign sources (Human Rights Council, 2013). For those charities involved in service activities, the vital element is to have access to resources. The resources can be in the form of donations, grants, sponsorship and social investment, while the restriction on resources can undermine the right to freedom of association. Although the right to association is not absolute or non-derogable, the restriction must be for 'the interests of national security or public safety, and public order' (ICCPR, 1996). One of the reasons to limit access to findings on the part of charities is protection from terrorism financing which might endanger national security. So, while the limitation might be regarded as being on legitimate grounds, it must be proportionate, necessary and proscribed by law. However, national security might be regarded as a justification in terms of 'suppressing opposition or to justify repressive practices against its population' (UNGA, 2006). In addition, some obligations, such as routing funding through state channels, reporting all funds received from foreign sources and how these are allocated or used, obtaining authorisation from the authorities to receive or use funds, all constitute a violation of the right to association (Human Rights Council, 2013). As an example, Tunisia, Egypt and Saudi Arabia received compliance condition with the FATF recommendation 8 but at the expense of civil society, while 85% of cases were rated as being non-compliant or partially compliant (Romaniuk and Keatinge, 2018).

Thus, no access to the formal financial system will undermine both the delivery of charitable work, transparency and public trust (Charity Commission, 2013). Fear of consequences will deny people access to legitimate services.

Virtual Currencies

As a new technology, virtual currencies (VCs) have attracted investment and could be an effective method for promoting financial inclusion (He et al, 2016; Baruri, 2016) because storing and managing VCs can be done without the limitations facing the banking system. The essential requirements are internet access, smartphone and maintaining a wallet. On the other hand, based on the Risk-Based Approach, VCs are at risk of being used for terrorist financing (FATF, 2015a). However, the use of VCs for this purpose, so far, has only been confirmed in a small number of cases, such as the Ali Shukri Amin case in which he used Twitter to provide instructions on how to use Bitcoin to finance ISIS (FATF, 2015b).

Since 2014, the FATF has issued several guidance publications to assist countries in managing the risks emanating from VCs. Due to the need for advanced technology and infrastructure, some countries prohibit the use of VCs such as Bitcoin, Litecoin, Zcash, and Ripple. However, they should also assess the impact of prohibition which drives users to making use of underground services with no monitoring or supervision tools (FATF, 2015a). Other countries such as the US, the UK, Germany, France, and Canada have recently started regulating VCs (Keatinge *et al*, 2018). In the case of the EU, following fifth Anti-Money Laundering Directive (AMLD5) (2018), wallet providers and exchangers must apply CDD, monitoring and STRs, and member states of the EU will have to bring into force national laws and regulations in compliance with the AMLD5 by 10 January 2020. The EU financial institutions are largely reluctant to provide services to VC businesses because of the lack of a strong regulatory position to date (Keatinge *et al*, 2018).

The main challenge associated with VCs relevant to this paper is anonymity or pseudonymity which targets the CTF preventive measures, in particular CDD, monitoring and STRs. Among the different kinds of VCs, decentralised convertible currencies (cryptocurrency) are regarded as a high-risk currency, and are 'particularly vulnerable' to the terrorism financing risk. Cryptocurrency is defined as math-based peer-to-peer virtual currencies that are protected by cryptography (private key) and which have no central authority and monitoring processes, such as would be provided by a Central Bank (FATF, 2014b). As an example, the Bitcoin protocol does not need or provide identification and verification of users, it does not have a central oversight body, no AML/CTF software is available to monitor and identify suspicious transactions, and it has a cross-border nature (FATF, 2014b). In fact, a user's identity is not visible, but the information about their transactions, such as dates, values, and the Bitcoin addresses (public key) are all accessible publicly on the blockchain (Keatinge *et al*, 2018).

The current anonymity of most cryptocurrencies makes it difficult to determine the identities of the persons involved (FATF, 2015a), while if they use anonymisers such as Darknet, Mixer and Tor as anonymising tools (FATF, 2014b), determining the identity of users might be impossible. At the current time, countries should require convertible exchangers to conduct CDD when establishing any business (FATF, 2015a). Exchangers are required to keep a record of information to identify the parties involved, such as an IP address, public key, the nature and date of the transaction, and the amount involved, all of which are easily accessible through the blockchain (FATF, 2015a). This preventive measure is limited only to convertible cryptocurrencies. The required CDD does not explicitly cover the exchange of one cryptocurrency for another. That means it may make it easier for users to undertake the conversion of one currency such as Bitcoin for privacy coins, without CDD, monitoring and STRs being applied at the point of exchange (keatinge *et al*, 2018).

The misuse of VCs for money laundering purposes has already been confirmed through the Liberty Reserve and Silk Road cases (Trautman, 2014), while using VCs for terrorism financing purposes depends on the several factors. Terrorist organisations need funds for five broad categories of activities. The first is operational: terrorist organisations need money for pre-surveillance with regard to proposed attacks, such as money for travel, vehicles, weapons, false identity documents and basic living expenses. The second is funds for propaganda and recruitment, including the exploitation of social media for the purpose of recruitment, such as publishing magazines, newspapers and websites. Examples includes ISIS's *Dabiq* and Al-Qaeda's *Inspirer* magazines in the Arabian Peninsula. The third category is related to the training of their forces, such as running training camps. The fourth is funds for salaries and member compensation, and compensation for their families, because the financial security of members and their families can help to support the ideology and operations. Finally, terrorist organisations require funds for social services, with the aim usually being to undermine the legitimacy of the existing government to demonstrate to target populations that the state is neglecting them. This helps them to build support and recruit more people (FATF, 2015b). For all the above-mentioned categories, cryptocurrency properties, namely anonymity, usability, security, acceptance, reliability and volume, are important in order to be used by terrorists. It seems that the current cryptocurrencies are not totally appropriate for terrorists to use due to a number of problems such as a lack of totally anonymity, technical sophistication, the threat of cyber-attack, difficulties in exchanging cryptocurrencies to fiat currencies (government-issued currency), instability of the market, and the potential increase in price (Dion-Schwarz *et al*, 2019). However, this trend might change in the future. Some factors which increase the feasibility of cryptocurrencies for terrorist use include the growth in the market, the widespread adoption of anonymous cryptocurrencies, and inconsistent regulatory oversight (Dion-Schwarz *et al*, 2019). If this happens, and the trend of CTF preventive measures which have been applied so far on sectors at risk of terrorism financing continues, and transfers to VCs, it will lead to financial exclusion. In future, the combination of high-risk, high compliance cost (PWC, 2014), technical sophistication, uncertainty and incomplete regulations might lead to financial exclusion, as currently many banks are unwilling to enter into business relationships with VC companies (PWC, 2014). It is important to adopt a proportionate approach to VCs in order not to preclude the progress of VCs as an advanced technology, because VCs have the potential to improve payment efficacy, reduce transaction costs, and facilitate international remittances (He *et al*, 2016). Policy-makers and regulators must be aware of, and learn from, the unintended consequences of CTF applied on banks, *hawala* networks and charities, in order to regulate and supervise VCs with attention being paid to promoting financial inclusion. Nonetheless, the assessment contained this section cannot go further because VCs and the regulations imposed on them, are at an infant stage.

Conclusion

The counter-terrorism financing regulations and policy must simultaneously be in line with human rights law and be effective. The second aspect of the CTF framework, which is the preventive measures relating to the three main sectors, in the form of the formal financial system, the informal financial systems, charities, and virtual currencies with regard to the risk of terrorism financing, might lead to a counter-productive CTF framework. This counterproductivity can be due to a low risk-appetite, de-risking, de-banking, financial exclusion, and using unregulated or less regulated and supervised financial systems. Financial exclusion is a focal point which results in ineffective counter-terrorism measures which are caused mostly by the formal financial sector, in particular the banking system. The strict CTF regulations on banks, such as CDD, monitoring and STRs, create an atmosphere of ambiguity and fear, and lead banks not to enter into business relationships with some customers, and excluding them from banking services. In fact, the strict CTF regulations undermine the commercial function of the banks because they must do more than required for banking. By considering banks as frontline policemen, a hostile business environment is created (Mugarura, 2014). The risk-based approach shifts responsibility for security decisions to the private sector (De Goede, 2018). As a result, the existence of regulated banks will drive terrorist financiers or money launderers to the less regulated or unregulated financial systems. The new era of financial exclusion is as a result of conflict between de-regulation and imposing the strict CTF regulations on banks, as a private sector which causes banks only pays attention to boosting shareholders' benefits, although they are licensed by society to render services to the meet the requirement of society. The outcome of this conflict has the same consequences of the previous era of financial exclusion, namely poverty and social exclusion, which leads to the creation of an ineffective counter-terrorism financing framework. Due to the need for extra expenditure for compliance with CTF regulations and policies, fear of fines and penalties, breaching international sanctions, and damage to their reputation, banks have cut off certain relationships in order to be safe. However, this causes financial exclusion, not only of individuals, but also of CBRs, MVTS, charities, and VCs.

Acknowledgements

I thank Professor Clive Walker and Professor Peter Whelan for their comments that greatly improved the manuscript.

Notes

[1] Afghanistan; Algeria; Angola; Bangladesh; Burkina Faso; Cambodia; Cameroon; China; Colombia; Congo, Dem. Rep.; Cote d'Ivoire; Ecuador; Egypt; Ethiopia; Ghana; Guatemala; India; Indonesia; Iran; Iraq; Kenya; Madagascar; Malawi; Mali; Morocco; Mozambique; Nepal; Niger; Nigeria; Pakistan; Peru; Philippines; Romania; Sri Lanka; Sudan; Tanzania; Thailand; Uganda; Ukraine; Uzbekistan; Vietnam; Yemen; and Zambia.
[2] Austria, Belgium, Canada, Finland, Italy, Israel, Sweden, Spain, Ireland, France, Portugal, Czech Republic, and the UK.
[3] Australia, Norway, Denmark, the US, and Germany.
[4] New Zealand and the Netherlands.
[5] Afghanistan, Bosnia and Herzegovina, Guyana, Iraq, Lao PDR, Syria, Uganda, Vanuatu, Yemen, Iran, and Democratic People's Republic of Korea (DPRK).
[6] European Commission, Regulation 2016/1675, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, 14 July 2016.
[7] Bangladesh, Brazil, China, Colombia, Cote d'Ivoire, DRC, Egypt, Ethiopia, India, Indonesia, Kenya, Mexico, Morocco, Mozambique, Myanmar, Nigeria, Pakistan, Peru, Philippines, Rwanda, South Africa, Vietnam, Tanzania, Turkey, and Zambia.
[8] Cote d'Ivoire, DRC, Kenya, Mozambique, Nigeria, Rwanda, Vietnam, Tanzania, Turkey, and Zambia.
[9] Brazil, Colombia, India, Mexico, Myanmar, Pakistan, Philippines, and South Africa.
[10] Bangladesh, China, Egypt, Ethiopia, Indonesia, Morocco, and Peru.
[11] IVTS concept is contested and called with different names namely, alternative remittance system, parallel banking, underground banking, informal remittance system. In general, these concepts refer to the financial service outside of the conventional and regulated financial institution systems.
[12] 34 responses were received from a wide range of charities with different incomes and most of them worked overseas.

References

Basel Committee, (2003), 'Guide to Account Opening and Customer Identification', available at https://www.bis.org/publ/bcbs85annex.htm (accessed 20 February 2018).

Baruri, P., (2016), 'Blockchain Powered Financial Inclusion', available at: http://pubdocs.worldbank.org/en/710961476811913780/Session-5C-Pani-Baruri-Blockchain-Financial-Inclusion-Pani.pdf (accessed 27 May 2019).

BBC, (2017), 'London Bridge attack: Timeline of British terror attacks' (19 June 2017) available at: https://www.bbc.co.uk/news/uk-40013040 (accessed 13 January 2019).

Biali, G., (2012), 'Know Your Customer or Not', *University of Toledo Law Review*, 43, 319-366.

Blake, S. and de Jong, E., 'Financial Exclusion: A Guide for Donors and Funders' (2008) (Report, Resolution Foundation and Friends Provident Foundation), available at: https://www.thinknpc.org/wp-content/uploads/2018/07/Short-changed.pdf (accessed 13 April 2019).

Carbo, S., Gardener, E., and Molyneux, P., (2007), 'Financial Exclusion in Europe', *Policy Money and Management,* 27 (1), 21-27.

Chaikin, D., (2009), 'How Effective Are Suspicious Transaction Reporting Systems?', *Journal of Money Laundering Control*, 12(3), 238-253.

Charity Commission for England and Wales, (2013), 'Protecting Charities from Harm: Compliance Toolkit', available at: https://www.gov.uk/government/collections/protecting-charities-from-harm-compliance-toolkit (accessed 23 February 2019).

Charity Commission for England and Wales, (2017), 'Risk to Charities from an Individual Associated with Terrorism' (Case Report), available at: https://www.gov.uk/government/publications/risks-to-charities-from-an-individual-associated-with-terrorism-mashoud-miah/risks-to-charities-from-an-individual-associated-with-terrorism-mashoud-miah (accessed 13 February 2018).

Charity Finance Group, (2018), 'Impact of Money Laundering and Counter-Terrorism Regulations on Charities', available at: https://cfg.org.uk/userfiles/documents/Policy%20documents/Impact%20of%20money%20laundering%20and%20counter-terrorism%20regulations%20on%20charities.pdf (accessed 15 February 2018).

Cooper, K., and Walker, C., (2016), 'Security from Terrorism Financing: Models of Delivery Applied to IVTS', *British Journal of Criminology*, 56, 1125-1145.

Dahabshiil Transfer Services Ltd v Barclays Bank Plc (2013) EWHC 3379 (Ch).

De Goede, M., (2018), 'Counter-Terrorism Financing Assemblages after 9/11', King, C., Walker, C., and Gurulé, J. (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Palgrave Macmillan, Switzerland.
De Goede, M., (2003), 'Hawala Discourses and War on Terrorist Finance', *Environment and Planning: Society and Space,* 21, 513-532.
Demirguc-Kunt, A., Klapper, L., Singer, D., Ansar, S., and Hess, j., (2018), The Global Findex Database 2017: Measuring Financial Inclusion and the Fintech Revolution, (World Bank Group) available at: https://globalfindex.worldbank.org/#GF-ReportChapters (accessed 25 February 2019).
Dion-Schwarz, C., Manheim, D., and Johnston, P., (2019), 'Terrorist Use of Cryptocurrencies: Technical and Organisational Barriers and Future Threat', Rand Corporation.
Disaster Emergency Committee, 'Getting Aid to Syria: Sanctions Issue for Banks and Humanitarian Agencies' available at: https://www.dec.org.uk/sites/default/files/pdf/getting_aid_to_syria.pdf (accessed 17 March 2019).
Edmond, T., (2017), 'Politically Exposed Persons Regime' (House of Commons Library, Briefing Paper No. 7376), available at: file:///C:/Users/lwzm/Downloads/CBP-7376.pdf (accessed 9 February 2018).
European Commission, (2016), Regulation 2016/1675, supplementing Directive (EU) 2015/849 of the European Parliament and of the Council by identifying high-risk third countries with strategic deficiencies, 14 July.
FATF, (2005), *ML and TF Typologies*, Paris.
FATF, (2012), *FATF Recommendations 2012*, Paris.
FATF, (2013a), *National ML and TF Risk Assessment*, Paris.
FATF, (2013b), *AML and CTF Measures and Financial Inclusion*, Paris.
FATF, (2013c), *Politically Exposed Persons*, Paris.
FATF, (2013d), *The Role of Hawala and Other Similar Service Providers in ML and TF*, Paris.
FATF, (2014a), 'FATF Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking', available at: http://www.fatf-gafi.org/publications/fatfgeneral/documents/rba-and-de-risking.html (accessed 3 January 2019).
FATF, (2014b), *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*, Paris.
FATF, (2015a), *Virtual Currencies: Guidance for a Risk-Based Approach*, Paris.
FATF, (2015b), *Emerging Terrorist Financing Risks*, Paris.
FATF, (2016), *Correspondent Banking Service*, Paris.
FATF, (2017), *AML and TF Measures and Financial Inclusion: With a Supplement on Customer Due Diligence,* Buenos Aires.
FCA, (2016), 'Access to Financial Services in the UK', (Occasional Paper 17), available at: https://www.fca.org.uk/publication/occasional-papers/occasional-paper-17.pdf (accessed 17 February 2019).
FCA, (2018), 'High-risk Customers, including PEPs', available at: https://www.fca.org.uk/firms/money-laundering-terrorist-financing/high-risk-customers-politically-exposed-persons (accessed 18 February 2019).
FSB, (2017), 'FSB Action Plan to Assess and Address the Decline in Correspondent Banking' (Report to G20 summit).
Fujii-Rajani, R., (2017), 'Money Remitters Left out in the Cold: Blanket De-Risking Policies, Counterterrorism and Government Intervention in New Zealand', *Auckland University Law Review*, 23, 204-234.
Goodway, N., (2014), 'Paying the Price for Sanctions' (Independent, 14 August), available at: https://www.independent.co.uk/news/business/analysis-and-features/paying-the-price-for-sanctions-the-customers-with-iranian-links-being-ditched-by-british-banks-9679692.html (accessed 19 November 2018).
He, D., Habermeier, K., Leckow, R., Haksar, V., Almeida, Y., Kashima, M., Kyriakos-Saad, N., Oura, H., Saadi Sedik, T., Stetsenko, N., and Verdugo-Yepes, C., (2016), Virtual Currencies and Beyond: Initial Considerations (IMF, Discussion Note SDN/16/03).
Howell, J., (2006), 'The Global War on Terror, Development and Civil Society', *Journal of International Development,* 18, 121-135.
HM Treasury, (2006), 'Thinking about Risk, Managing your Risk Appetite: A Practitioner's Guide', available at: https://webarchive.nationalarchives.gov.uk/20130107005526/http://www.hm-treasury.gov.uk/d/tar_practitioners_guide.pdf (accessed 15 March 2019).
HM Treasury, (2007), 'The Financial Challenge to Crime and Terrorism', available at: http://webarchive.nationalarchives.gov.uk/+/http:/www.hmtreasury.gov.uk/media/C/B/financialchallenge_crime_280207.pdf (accessed 5 April 2018).
HM Government and Beechwood International, (2013), 'Safer Corridors: Rapid Assessment, Case Study: Somalia and UK banking', available at: www.gov.uk/government/uploads/system/uploads/at

tachment_data/file/283826/SAFER_CORRIDORS_RAPID_ASSESSMENT__2013__SOMALIA__UK_BANKING.PDF/ (accessed 24 December 2018).
Human Rights Council, (2013), 'Report of the Special Rapporteur of the Rights to Freedom of Peaceful Assembly and of Association', Maina Kiai, A/HRC/23/39.
ICJ, (2018), *Islamic Republic of Iran v. United States of America*, 'Alleged Violations of the 1955 Treaty of Amity, Economic Relations, and Consular Rights: Request for the Indication of Provisional Measures', ICJ, No. 175.
Immigration and Refugee Board of Canada, (2015), 'Somalia: Prevalence and availability of institutions that conduct Hawala transfers both into an out of Somalia; documents or identification needed to use a remittance company (Hawala); whether they deal with institutions operating in Ethiopia or Kenya', available at: https://www.refworld.org/docid/551d07494.html (accessed 23 April 2019).
IMF, (2016), 'The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action', available at: www.imf.org/external/pubs/ft/sdn/2016/sdn1606.pdf (accessed 27 December 2018).
ITU, (2016), 'Review of National Identity Programs', available at: https://www.itu.int/en/ITU-T/focusgroups/dfs/Documents/09_2016/Review%20of%20National%20Identity%20Programs.pdf (accessed 5 April 2019).
Joint Money Laundering Steering Group Official Website, available at: http://www.jmlsg.org.uk.
Joint Money Laundering Steering Group, (2017), 'Prevention of Money Laundering/ Combating Terrorist Financing' (Guidance).
Kamali Dehghan, S., (2017), 'UK Bank Accounts of Iranian Customers still Being Closed, Says Law Firm', (Guardian, 21 April) available at: https://www.theguardian.com/money/iran-blog/2017/apr/21/law-firm-reports-surge-in-iranians-uk-bank-accounts-being-closed-sanctions-iran-nuclear-deal-trump (accessed 19 November 2018).
Keatinge, T., (2014a), *Counter Terrorist Regulation Restricts Charity Worldwide: Uncharitable Behaviour,* Demos.
Keatinge, T., (2014b), 'Breaking the Banks: The Financial Consequences of Counterterrorism', *Foreign Affairs.*
Keatinge. T., Carlisle, D., and Keen, F., (2018), 'Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses' (European Parliament).
Koker, L., (2006), 'ML Control and Suppression of Financing of Terrorism', *Journal of Financial Crime,* 13(1), 26-50.
Koker, L., (2011),'Aligning Anti-Money Laundering, Combating of Financing of Terrorism and Financial Inclusion: Questions to Consider When FATF Standards Are Clarified', *Journal of Financial Crime,* 18 (4), 361-386.
Koku, P.S., (2009), 'Doing Well by Doing Good – Marketing Strategy to Help the Poor: The Case of Commerce Banks in Ghana', *Financial Services Marketing,* 41(2), 135-151.
Koku, P.S., (2015), 'Financial Exclusion of the Poor: A Literature Review', *International Journal of Bank Marketing*, 33(5), 654-668.
Lafolla, V., 'The Production of Suspicious in Retail Banking: An Examination of Unusual Transaction Reporting', King C., Walker C., and Gurulé J. (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Palgrave Macmillan, Switzerland.
Law Commission, (2018), 'Anti-Money Laundering: the SARs Regime' (Consultation Paper No 236).
Magazine for Career-Minded Professionals in the Anti-Money Laundering Field, (2017), 'De-Risking and Financial Inclusion', available at: https://www.acamstoday.org/de-risking-and-financial-inclusion/ (accessed 12 May 2019).
Mugarura, N., (2014), 'Customer Due Diligence Mandate and the Propensity of its Application as a Global AML Paradigm', *Journal of Money Laundering Control*, 17 (1), 76-95.
Nicoli M., (2018), 'De-risking and Remittances: The Myth of the Underlying Transaction Debunked', (World Bank), available at: http://blogs.worldbank.org/psd/de-risking-and-remittances-myth-underlying-transactiondebunked (accessed March 2019)
Pantuliano, S., Mackintosh, K., Elhawary, S., and Metcalfe, V., (2011), 'Counter-Terrorism and humanitarian Action: Tensions, Impact and Ways Forward' (Humanitarian Policy Group, Policy Brief 43).
Gordon, S., and Taraboulsi-McCarthy, S., (2018), 'Counter-terrorism, Bank De-Risking and Humanitarian Response: A Path Forward' (Humanitarian Policy Group, Policy Brief 72)
Passas N., (1999), 'Informal Value Transfer Systems and Criminal Organizations: A Study into So-Called Underground Banking Systems' (WODC).
PWC, (2014), 'Virtual Currencies: Out of the Deep Web, into the Light', available at: https://www.pwc.com/im/en/publications/assets/banking/pwc_virtual_currencies_risk_opportunities.pdf (accessed 24 May 2019).
Ramachandran V., (2015), 'Unintended Consequences of Anti-Money Laundering Policies for Poor Countries', (Centre for Global Development Working Group Report), available at:

www.cgdev.org/sites/default/files/CGD-WG-Report-Unintended-Consequences-AML-Policies-2015.pdf (accessed 21 December 2018).
Ramachandran V., Collin, M., and Juden, M., (2018), 'De- risking: An Unintended Negative Consequence of AML/CFT Regulation', King, C., Walker, C., and Gurulé, J. (eds.), *The Palgrave Handbook of Criminal and Terrorism Financing Law*, Palgrave Macmillan.
Reuters, (2019), 'Flood-Hit Iran Getting no Financial Aid from Abroad due to US Sanctions' (7 April) available at: https://www.reuters.com/article/us-iran-floods-redcrescent/flood-hit-iran-getting-no-financial-aid-from-abroad-due-to-u-s-sanctions-statement-idUSKCN1RJ0GY (accessed 22 April 2019).
Romaniuk, P., and Keatinge, T., (2018), 'Protection Charities from Terrorist and Counter-terrorists: FATF and the Global Effort to Prevent Terrorist Financing through the Non-Profit Sector', *Crime Law Social Change*, 69 (2), 256-282.
Razavy, M., (2005), 'Hawala: An Underground Haven for Terrorists or Social Phenomenon?', *Crime, Law and Social Change,* 44(3), 277-299.
Sambei, A., Plessis, A., and Polaine, M., (2009), *Counter-Terrorism Law and Practice: An International Handbook*, Oxford University Press, Oxford.
Shehu, Y., (2012), 'Promoting Financial Inclusion for Effective Anti-Money Laundering and Counter Financing of Terrorism (AML/CFT)', *Criminal Law Society Change,* 57, 305-323.
Solo, M.T., (2008), 'Financial Exclusion in Latin America – or the Social Costs of not Banking the Urban Poor', *Environment and Urbanization*, 20 (1), 47-66.
Stanley, R., and Buckley, R., (2016), 'Protecting the West, Excluding the Rest: The Impact of the AML/CTF Regime on Financial Inclusion in the Pacific and Potential Responses, *Melbourne Journal of International Law,* 17, 83-105.
Trautman, L., (2014), 'Virtual Currencies Bitcoin and What Now after Liberty Reserve, Silk Road and Mt. Gox?', *Richmond Journal of Law and Technology*, 20 (4), 13-14.
Trausolt, J., and Johnson, J., (2012), 'International Anti-Money Laundering Regulation of ARS: Why the Current Approach Does not Work in Developing Countries', *Journal of Money Laundering Control*, 15 (4), 407-420.
Metcalfe-Hough, V., Keatinge, T., and Pantuliano, S., (2015), 'UK Humanitarian Aid in the Age of Counter-Terrorism: Perceptions and Reality' (Working paper, Overseas Development Institute).
UN, (2019), 'SC Unanimously Adopts Resolution Calling upon Member States to Combat, Criminalise Financing of Terrorists, Their Activities', (Meeting Coverage and Press Release, 28 March 2019) available at: https://www.un.org/press/en/2019/sc13754.doc.htm (accessed 29 March 2019).
UNDP, 'Sustainable Development Goals' available at: http://www.undp.org/content/undp/en/home/sustainable-development-goals.html (accessed 25 December 2018).
UNICEF, (2013), 'Final Evaluation of the Unconditional Cash and Voucher Response to the 2011-12 Crisis in Southern and Central Somalia'.
UNGA, (1966), International Covenant on Civil and Political Rights (ICCPR) (1966), Res 2200A (XXI),16 December.
UNGA, (1999), 'International Convention for the Suppression of the Financing of Terrorism (1999)', Res 54/109, 9 December 1999, art 18 (1)(b).
UNGA, (2006), 'Protection of Human Rights and Fundamental Freedoms While Countering Terrorism', UN. Doc A/61/267.
UNSC, (2001), Res 1373 (2001), UN Doc. S/RES/1373, 28 September.
UK National Crime Agency, (2017), 'Suspicious Activity Reports' (Annual Report), available at: http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/826-suspicious-activity-reports-annual-report-2017/file (accessed 11 February 2019).
UK National Crime Agency, (2018), 'Suspicious Activity Reports' (Annual Report), available at: http://www.nationalcrimeagency.gov.uk/publications/suspicious-activity-reports-sars/992-2018-sars-annual-report/file (accessed 11 February 2019).
Walker, C., (2014),'Terrorism Financing and the Policy of Charities: Who Pays the Price?', King, C., and Walker, C., (eds), *Dirty Assets: Emerging Issues in the Regulation of Criminal and Terrorist Assets*, Ashgate.
World Bank, (2008) 'Finance for All? Policies and Pitfalls in Expanding Access'.
World Bank, (2020), 'Universal Financial Access 2020'.
World Bank, (2015), 'Group Withdrawal from Correspondent Banking: Where, Why, and What to Do About it (Working Paper 101098).
World Bank, (2015), 'Report on the G20 Survey on De-Risking Activities in the Remittance Market'.