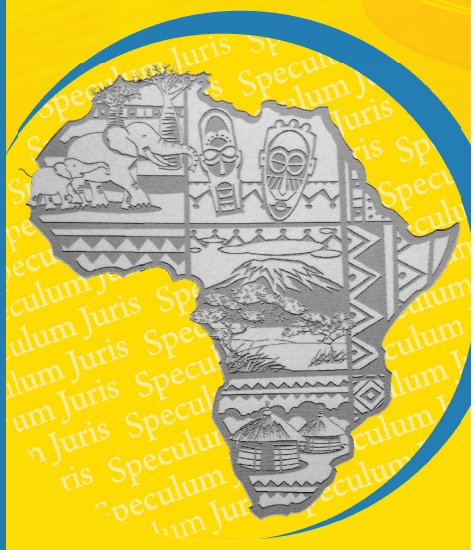
Speculum Juris

Special Issue on Confronting the Effects of the COVID-19 Pandemic on Corporate Governance, Corporate Insolvency and Financial Education Measures in Practice

Guest Editor
Prof Howard Chitimira

Vol 36 No 2 (2022)
Published 30 December 2022

ISSN 2523-2177



Cite as: Tongoi "A Perspective on Post-Pandemic Implications of Criminal Abuse and Money Laundering on Mobile Financial Services" 2022 (36) Spec Juris 233–255

University of Fort Hare
Together in Excellence

A Perspective on Post-Pandemic Implications of Criminal Abuse and Money Laundering on Mobile Financial Services

Edwin AA Tongoi*
Lecturer, Australian Graduate School of Policing and Security, Charles Sturt University, Australia

Abstract

Due to the COVID-19 pandemic, global standard-setting bodies encouraged new contactless payments, to minimise the threat posed by the virus and to advance financial inclusion. The features of mobile financial services (MFSs) as a related payment method, are potentially attractive to criminals who wish to conceal proceeds of crime and launder funds through mainstream payment systems that are now interoperable with the mobile payment systems. In the aftermath of the pandemic, it is crucial to address regulatory concerns to safeguard the system and minimise this threat. This article draws on the Financial Action Task Force (FATF) standards and assesses the potential role of MFSs in money laundering and terrorism financing. It identifies obstacles that could limit the efficacy of a harmonised anti-money laundering and counter-terrorist financing (AML/CFT) policy in jurisdictions where MFSs have taken form. It evaluates the challenges of contextually complying with the international approach to combating money laundering and financing terrorism. Further, it highlights the requisite global AML/CFT standards and draws attention to the growing risk of criminal abuse of MFSs where global standards may not be uniformly applied.

* BA (PU); LLB (Poona); Dip Law (KSL); MCom Law; PhD (Deakin).

The article concludes by highlighting specific areas that require adjustment to safeguard MFSs from criminal abuse.

Keywords: Mobile financial services; mobile money; money laundering; terrorist financing

1 INTRODUCTION

The COVID-19 pandemic has drawn attention to the urgent need to digitise transactions in many jurisdictions that were yet to make progress in adopting the digital economy. Most countries have made some progress toward this, but this may not be enough. At the heart of this economy is the ability to transact in a way that allows for value to be moved to and from an increasing number of participants, many of whom have had to rapidly shift operations to online platforms to remain in business, on account of the restrictions and constraints that the pandemic brought. Digital financial services are therefore now arguably in the greater spotlight and there is an urgency to ensure that all the aspects necessary to facilitate the entrenchment of the digital economy are in place. Mobile financial services (MFSs) are an integral part of this process. MFSs are characterised by speed and convenience. Funds can be transferred by subscribers in different parts of the world, in real-time and with relative anonymity, from an enabled mobile money account, regardless of geographical boundaries. This is largely facilitated by the use of smartphones, as opposed to feature phones, which may not be as efficacious. MFSs also have the capacity to draw in an increasing number of unbanked or underbanked people. Whilst they thus clearly advance the inclusion agenda, MFSs are of increasing concern as they are a potentially attractive channel for abuse by criminals wishing to disguise the proceeds of crime and/or introduce illegitimately obtained funds into mainstream circulation.[1] The Financial Action Task Force (FATF) has recognised the challenge posed by the global pandemic and has urged governments, financial institutions, and other businesses to remain alert to "new and emerging illicit finance risks".[2] MFSs are nonetheless a channel that can bring great economic development and an improvement in the lives of users who benefit from the low transaction costs and greater access to financial services.[3] The benefits that accrue to users may also serve as an incentive for criminals to misuse the channel. With increased economic activity being channelled through MFSs and the resultant potential abuse, it is critically important to ensure the adequacy of regulation, for purposes of preserving the integrity of the system, by preventing money laundering and the financing of terrorism, which can both be committed through the MFSs infrastructure.

This article draws on the standards set by the FATF and assesses the potential role of MFSs in money laundering and terrorism financing and the related risk. It proceeds to identify obstacles that could limit the efficacy of a harmonised anti-money laundering and countering the financing of terrorism (AML/CFT) policy in jurisdictions where MFSs are well developed. It evaluates the challenges faced in the MFSs environment in the process of contextually complying with the international approach to combating money laundering and financing of terrorism. Further, it highlights the global AML/CFT standards that countries are required to meet and

1 Vlcek "Global Anti-Money Laundering Standards and Developing Economies: The Regulation of Mobile Money" 2011 *Development Policy Review* 415 416; De Koker "The 2012 Revised FATF Recommendations: Assessing and Mitigating Mobile Money Integrity Risks Within the New Standards Framework" 2013 *Wash. J.L. Tech. & Arts* 165 188.

2 FATF "Statement by the FATF President: COVID-19 and Measures to Combat Illicit Financing" 2020 https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html (accessed 03-08-2021).

3 Cull, Ehrbeck, Holle "Financial Inclusion and Development: Recent Impact Evidence" (2014) https://www.cgap.org/sites/default/files/FocusNote-Financial-Inclusion-and-Development-April-2014.pdf (accessed 01-05-2021).

draws attention to the growing risk of criminal abuse of MFSs in an environment where global standards may not be uniformly applied. The article concludes by suggesting specific areas that require adjustment for purposes of safeguarding MFSs from criminal abuse.

2 DEFINING MONEY LAUNDERING AND TERRORISM FINANCING

2 1 Money Laundering and its Stages

Money laundering is the clandestine injection of illegitimately obtained funds into legitimate payment channels, with the aim of creating the impression that the funds have in fact been obtained legally. The real source of the funds is concealed, and the criminals look to gain undetected access to the funds through legitimate channels. It enables the growth of organised crime through the actions of criminals who wish to *legitimise* their illegally acquired money and assets.[4] The early usage of the term "money laundering" can be traced back to activities in the mid-1970s when it is said to have been coined by American law enforcement agencies and was popularly used during the Watergate inquiry.[5] It appears to have first been used formally in 1982 in the case of *United States v. $4,255,625.39 (1982) 551F Supp 314*. Money laundering was established as a domestic felony in the United States in 1986 and was thereafter championed through the G7 group of countries, a process that eventually led to the formation of the FATF in 1989.[6] It was formally acknowledged in Vienna, on the adoption of the United Nations Convention Against Illicit Traffic In Narcotic Drugs and Psychotropic Substances, (Vienna Convention) on 19 December 1988, which required the creation of the criminal offence of money laundering by Member States.[7] With 87 signatories to the Convention and 191 parties,[8] there has been near universal acceptance of the need to address this criminal activity and many countries have now domesticated the provisions into their laws. Similarly, the United Nations Convention against Transnational Organized Crime[9] (Palermo Convention) and the United Nations Convention against Corruption[10] (Merida Convention) require member states to establish money laundering as a criminal offence. The desired effect of criminalising money laundering is to prevent the enjoyment of illegitimately obtained funds by criminals and the discouragement of predicate offences.[11]

Whilst there is a nuanced approach to the domestication of the money laundering offence in different jurisdictions, there is some commonality with which various scholars have defined money laundering. Brigitte Unger defines it as "the process of disguising the unlawful source of criminally derived proceeds to make them appear legal".[12] Angela Veng Mei Leong defines it as

4 Durrieu *Rethinking Money Laundering and Financing of Terrorism in International Law: Towards a New Global Legal Order* (2013); Buchanan "Money Laundering—A Global Obstacle" 2004 *Research in International Business and Finance* 115.

5 Gilmore *Dirty Money: The Evolution of International Measures to Counter Money Laundering and the Financing of Terrorism* (2004) 20.

6 Vlcek 2011 *DPR* 417; Financial Action Task Force "History of the FATF" http://www.fatf-gafi.org/about/historyofthefatf/#d.en.3157 (accessed 02-05-2021).

7 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Treaty Series, vol. 1582, UN ESCOR, UN Doc E/CONF.82/15 (10 December 1988) Art 3.

8 See United Nations "Chapter VI Narcotic Drugs and Psychotropic Substances, 'Depositary'" https://treaties.un.org/Pages/ViewDetails.aspx?src=IND&mtdsg_no=VI-19&chapter=6&clang=_en (accessed on 02-05-2021).

9 Article 6 and Article 7.

10 Article 14.

11 Stessens *Money Laundering: A New International Law Enforcement Model* (2000) 12.

12 Durrieu *Rethinking Money Laundering* 15, citing Unger "*The Scale and Impacts of Money Laundering*" (2007) 15.

"a process that employs financial accounting, legal and other instruments in conjunction with an object that has either been used in, or derived from, unlawful activity" aimed at "create[ing] a veil of legal cleanliness around the object".[13] According to William R. Shroeder, it is "the process by which one conceals the existence, illegal source, or illegal application of income and then disguises that income to make it appear legitimate".[14] Adam Graycar and Peter Grabosky define it as "the process by which the proceeds of crime are put through a series of transactions, which disguise their illicit origins, and make them appear to have come from a legitimate source".[15] The FATF broadly defines money laundering as the processing of the proceeds of crime to disguise their illegal origin.[16] The United Nations Office on Drugs and Crime (UNODC), in its definition, also places some emphasis on the concealment of the origins of earnings from illegal sources, to give the impression that they are from lawful sources.[17]

Money laundering is conventionally perceived as a process but may also be an event. It is much more than the mere disguising of unlawful sources of criminal proceeds and can also be committed without necessarily going through a series of transactions.[18] It involves the use of existing financial tools and infrastructure to legitimise ill-gotten gains. These tools and infrastructure are often prone to change as a result of advancements in technology. The definitions cited above clearly highlight the need for concealment of the source of funds or the assets and, similarly, the need for a predicate offence to satisfy the elements of the offence of money laundering as envisaged. Where the aspect of concealment is lacking, courts have held that the offence of money laundering was not established.[19] It is therefore crucial that, in defining the offence in domestic legislation, there should be clarity in what a predicate offence is. In its interpretive note to Recommendation 3, the FATF recommends that predicate offences be

> described by reference to all offences; or to a threshold linked either to a category of serious offences; or to the penalty of imprisonment applicable to the predicate offence (threshold approach); or to a list of predicate offences; or a combination of these approaches.[20]

The approach taken by each jurisdiction would therefore determine the reach of the money-laundering offence.

Money laundering can be committed across multiple jurisdictions, in furtherance of the concealment of the illegitimate sources.[21] The financial tools and infrastructure that currently exist can facilitate this with alarming speed. It is in this context that MFSs, with their associated speed and complexity, are considered to be an avenue that may enable money laundering across multiple jurisdictions. This is testimony to the challenge faced by different jurisdictions in keeping up with the creativity and adeptness of criminals who may seek to exploit this

13 Durrieu *Rethinking Money Laundering* 15, citing Leong "*The Disruption of International Organised Crime: An Analysis of Legal and Non-Legal Strategies*" (2007) 31.

14 Schroeder "Money Laundering - A Global Threat and the International Community's Response" 2001 *FBI Law Enforcement Bulletin* 1.

15 Graycar and Grabosky "*Money Laundering in the 21st Century: Risks and Countermeasures*" (1996) 2 viii.

16 Financial Action Task Force "What is Money Laundering?" http://www.fatf-gafi.org/faq/moneylaundering/#d.en.11223 (accessed 01-02-2018).

17 United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances art 3.

18 De Koker *et al. Money Laundering and Terror Financing: Law and Compliance in South Africa* (2022) 5.

19 See *Thales South Africa (Pty) Ltd v National Director of Public Prosecutions* N.O and [2021] 2 All SA 274 (KZP) para 83.

20 Financial Action Task Force "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" 38.

21 Council Directive 91/308/EEC of 10 June 1991 on Prevention of the Use of the Financial System for the Purpose of Money Laundering 1991 (OJ L) Recital 6.

fast changing and increasingly accepted means of moving money; by gaining access to it without attracting the attention of law enforcement, more so in an environment where cashless transactions are now encouraged for purposes of achieving various pandemic-related goals.

Some scholars have emphasised the aspect of access and enjoyment of proceeds of crime, or their conversion into a form that allows launderers the power to make purchases, as being important in the laundering process.[22] It therefore follows that definitions which do not lay similar emphasis arguably do not depict the full process.[23] Whilst recognising that not all money laundering schemes unfold through specific conventionally known stages, there are arguably not less than three known stages that characterise the process in many such schemes as set out hereafter.[24]

2 1 1 Stage 1 – Concealment

The first stage involves the concealment or placement of illegitimately obtained funds. The funds are put into mainstream financial systems as inconspicuously as possible, to minimise any suspicions as to their source. This may be done directly by the criminals or through third parties.

2 1 2 Stage 2 – Layering

This stage is referred to as layering or converting. It entails the deliberate movement or transfer of funds between various locations, sometimes through multiple transactions, with the intention of convoluting the process that would track such funds or any resultant audit trail. This would make it especially difficult to determine the origin of funds and is designed to evade reporting obligations that are placed by industry regulators. A common method of moving funds in this way is by using several recruits who move the money around for a fee, whilst ensuring that no reporting thresholds are triggered.[25] This is referred to as smurfing and the recruits would be termed "smurfs" or "money mules".[26] Criminals have been known to exercise a lot of patience with this process and have in fact been understood to work in groups, to transit funds through what may be perceived as low-risk channels from emerging new payment products and services.[27]

2 1 3 Stage 3 – Integration

In this stage, funds that are now ostensibly legitimate are accessed for purposes of investment or for consumption. This would ordinarily be through the mainstream financial system or economy.

2 1 4 Stage 4 – Legitimisation

This stage is not formally recognised but involves ascertaining the success of the laundering process and is often included in the third stage.

---

22 Stessens 83; Masciandaro "*Economics of Money Laundering: A Primer*" (2007) 2 https://pdfs.semanticscholar.org/b0c7/21177c5b827740086f5093a47e122a9f6b27.pdf?_ga=2.230531487.208205085.1571118939-303168498.1571118939 (accessed 02-05-2021); Buchanan 2004 117.

23 Tongoi *Mobile Financial Services: Regulatory Responses — Kenya, South Africa and Australia* (PhD Thesis, Deakin University, 2020).

24 Financial Action Task Force "What is Money Laundering?" para 9–11; Irwin, Choo and Liu "An Analysis of Money Laundering and Terrorism Financing Typologies" 2012 *Journal of Money Laundering Control* 85, 87; Stessens 84; Buchanan 2004 117 para 2–5.

25 Zhdanova *et al.* "No Smurfs: Revealing Fraud Chains in Mobile Money Transfers" (*International Conference on Availability, Reliability and Security,* 2014) 11, 12; Chatain *et al. Protecting Mobile Money Against Financial Crime: Global Policy Challenges and Solutions* (2011) 35.

26 Zhdanova *et al.* 2014 11.

27 De Koker 2013 *WJLTA* 188.

2 2 Jurisdictional Definitions of Money Laundering

As a result of different jurisdictional approaches taken in domesticating the term, definitions of money laundering vary globally.[28] Under Recommendation 3 of the FATF Recommendations,[29] however, the criminalisation of the offence should be "on the basis of the Vienna Convention and the Palermo Convention"[30] and as such, the differences continue to lessen. The interpretation and more traditional use of the term would entail a description or depiction of a process where proceeds of crime are deliberately subjected to a series of transactions to hide or disguise their illicit origin and give them the appearance of legitimacy. Domestication is invariably based on the process and interpretation that each country adopts and there is yet to be definitional universality of the term *money laundering*. To the extent that countries should use the Vienna Convention and the Palermo Convention as the basis of such domestication, global definitions will vary on account of different jurisdictions having had to suit the definitions to their individual circumstances.

Illustratively, the South African definition of money laundering is:

> an activity which has or is likely to have the effect of concealing or disguising the nature, source, location, disposition or movement of the proceeds of unlawful activities or any interest which anyone has in such proceeds, and includes any activity which constitutes an offence in terms of section 64 of [FICA] or section 4, 5 or 6 of [POCA].[31]

There is a focus on the proceeds of unlawful activities which, as a result of and based on how "proceeds" is defined, has been criticised in some quarters as being capable of circumvention by interpreting the term to mean "only benefits which were *generated* by unlawful activities as opposed to benefits which were *acquired* through unlawful activities".[32] Arguably, the concern is mitigated by the definition of "proceeds of unlawful activities" under the Prevention of Organised Crime Act[33] as:

> any property or any service, advantage, benefit or reward which was derived, received or retained, directly or indirectly, in the Republic or elsewhere, at any time before or after the commencement of this Act, in connection with or as a result of any unlawful activity carried on by any person, and includes any property representing property so derived.[34]

This act goes on to set out the offences relating to proceeds of unlawful activities in its sections 4, 5 and 6 by criminalising the dealing with property in the knowledge, imputed or otherwise, that it may be part of the proceeds of unlawful activities, assisting another to benefit from proceeds of crime and the acquisition, possession, or use of proceeds of unlawful activities.

The Australian approach in the Anti-Money Laundering and Counter-Terrorism Financing Act[35] defines money laundering with reference to the Criminal Code. The Criminal Code defines it

28 Durrieu *Rethinking Money Laundering* 13–17; Buchanan 2004 117; Institute of International Finance "Deploying Regtech Against Financial Crime" 13 https://www.iif.com/portals/0/Files/private/32370132_aml_final_id.pdf (accessed 09-08-2021).

29 The relevant Recommendations in the MFSs context are addressed in greater detail in a subsequent part of this article at para 4.1.

30 Financial Action Task Force "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" 3.

31 Financial Intelligence Centre Act 2001 s 1.

32 Jaarsveld *Aspects of Money Laundering in South African Law* (LL.D Thesis, University of South Africa, 2011) 200 468.

33 121 of 1998.

34 Section 1.

35 No. 169, 2006 (Cth).

in a rather complex manner by the creation of nineteen different offences.[36] These are largely categorised as "those that have a link to the proceeds of crime or generated by illegal activity and those that have a link to the instruments of the crime or the funds used to conduct the activity."[37] Under the code, possession of the proceeds or instruments of crime is a single offence. It is also an offence for persons to receive, possess, conceal, import into Australia, export from Australia, or dispose of, the proceeds of crime.[38] The code also creates offences relating to dealing with the proceeds or instruments of crime, where possessing proceeds of crime and engaging in banking transactions involving those funds, is an offence. Each of the offences have a component of knowledge, recklessness, and negligence in each band of the established offences[39] and have a broad and wide reach.[40]

2 3 Financing of Terrorism

With the acts of terror that happened in the United States of America on 11 September 2001, global policy makers began to link money laundering and financing of terrorism. The FATF expanded its anti-money laundering recommendations and inserted a further Nine Special Recommendations on terrorism financing.[41] Security Council Resolution 1373 was also passed by the United Nations and adopted unanimously on 28 September 2001.[42] This resolution bound Member States to domestically criminalise acts of terror.

In contrast to money laundering, where the flow of funds is from illegitimate sources to legitimate financial systems, the flow of funds in the financing of terrorism will often be from both legitimate and illegitimate sources, to fund illegitimate acts of terror.[43] Both money laundering and the financing of terror ultimately give the offenders access to funds. It is however significantly more difficult to track the methods used by terror groups to move their funds, especially because these funds may in fact be drawn from legitimate sources[44] and will not always be transferred in large quantities. Recent acts of terror on the global landscape have shown that even small amounts of money may well be all a terrorist needs to be able to give effect to an act of terror. The funds may be, but need not be, channelled through illegitimate sources.

2 3 1 Defining Terrorism

The definition of the term "terrorism" is yet to achieve universal concurrence.[45] The terms "act of terror" and "financing terrorism" have, however, found some definitional concurrence. In the perspective of the World Bank and the International Monetary Fund, financing of terrorism is deemed to be the provision of "financial support for terrorism or for those who encourage,

36 Criminal Code Act 1995 (Cth) div 400.

37 Tongoi *Mobile Financial Services* 212.

38 Criminal Code Act 1995 (Cth) s 400.2.

39 Criminal Code Act 1995 (Cth) ss 400.3–400.8.

40 Tongoi *Mobile Financial Services* 213.

41 De Koker 2013 WJLTA 172; Financial Action Task Force "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" (2012-2021) 6 http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%20 2012.pdf (accessed 31-08-2021).

42 United Nations Security Council Resolution 1373 (2001) https://undocs.org/S/RES/1373(2001) (accessed 09-10-2019).

43 Durrieu *Rethinking Money Laundering* 70–71.

44 Irwin, Choo and Liu 2012 *JMLC 88*; Schott *Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism* (2006).

45 Durrieu *Rethinking Money Laundering* 66 para 4.

plan, or engage in terrorism".[46] The FATF does not provide its own definition[47] but relies on the one in the International Convention for the Suppression of the Financing of Terrorism, adopted by the United Nations in 1999 ("Terrorist Financing Convention"),[48] which defines the financing of terrorism as being where "a person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out" an act of terror.[49] It goes on to define "acts of terror" to be acts which are so designated by the various treaties that are listed by the convention, or acts which are "intended to cause death or serious bodily injury" to civilians or other persons not actively involved in armed conflict, with the purpose of intimidating a population, or forcing "a government or an international organisation to do or to abstain from doing an act".[50]

3 MFSs AND THEIR ROLE IN MONEY LAUNDERING AND TERRORISM FINANCING

3 1 The Mobile Money Transaction and its Vulnerability

The hidden nature of money laundering and terrorist financing activity make the task of quantifying the actual sums involved extremely difficult. Estimates by the UNODC put the annual figure of money laundered globally at "2 – 5% of global GDP, or $800 billion – $2 trillion in current US dollars".[51] Determining how much of these sums are channelled through MFSs is even more problematic. In comparison to other methods of channelling funds, there is little evidence yet that MFSs have been a key channel for money laundering and terrorist financing.[52] However, the affordances of the MFSs ecosystem and the heterogeneity of stakeholders make the whole system vulnerable to criminal misuse and abuse. It may be argued that criminals are less likely to trust technology on account of the potential for surveillance and, in this context, the variety of data collectable through the MFSs ecosystem. It may also be argued in the converse that where the perception is that surveillance is likely to be low, criminals may nonetheless exploit the technology to their advantage.[53] The speed and convenience that allow for real time transfer of mobile money outside of mainstream financial payment systems, coupled with anonymity, are as attractive a feature to criminal elements as they are to legitimate users. Where smartphones are used, these transactions can also be concluded across jurisdictions where regulation may differ and may provide some benefit for criminals, depending on their location. The typical transaction would permit the movement of funds from legitimate activity in one jurisdiction to another. Such activity may be criminalised in the other jurisdiction and therefore be subject to proceeds of crime interpretation, but the movement of funds, in and of itself, will not divulge

46 Durrieu *Rethinking Money Laundering* 68; Schott *Reference Guide to Anti-Money Laundering* I-1.

47 Schott *Reference Guide to Anti-Money Laundering* I-5.

48 *International Convention for the Suppression of the Financing of Terrorism* https://www.un.org/law/cod/finterr.htm (accessed 02-06-2018).

49 *International Convention for the Suppression of the Financing of Terrorism* Art 2(1).

50 *Ibid*.

51 United Nations Office on Drugs and Crime "Money Laundering" https://www.unodc.org/unodc/en/money-laundering/overview.html (accessed 10-09-2021).

52 Solin and Zerzan Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks (2010) 9 https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2012/06/amlfinal58.pdf (accessed 03-05-2021).

53 The recent Operation Ironside that enabled law enforcement agencies to lead organised crime groups into believing and therefore freely using an encrypted messaging app called Anom, which was secretly controlled by the FBI is a case in point. See: Farzan and Taylor "What is Anom, and how did law enforcement use it to arrest hundreds in a global sting?" *The Washington Post* (8 June 2021).

the emanating activity outside of the transaction monitoring that occurs within the ecosystem.

Mobile money transactions typically require a mobile communications service[54] ordinarily provided by a Mobile Network Operator (MNO).[55] The MFSs ecosystem may be led by an MNO or by a financial institution, or it may in fact be a hybrid where third parties are required to partner with banks and/or MNOs.[56] The MNO-led variation[57] is more prevalent in emerging markets. The model that is adopted to deploy MFSs depends on the domestic regulatory environment. In the MNO-led model the infrastructure is created and managed by the MNO and access to the payment system is based on a periodical subscription fee, payable by users and effected through an interface that enables various transactions. Through a customer interface[58] subscribers and service providers interact with each other by exchanging data and value to complete the mobile money transaction. The transaction processing[59] phase allows for issuance of instructions for the movement of information and/or value to a specific destination, which then permits access by the recipient. The value that is exchanged is stored electronically but maintained through a banking institution, where a specific account is held on behalf of the MNO, in the case of mobile money transactions. The entry is stored electronically in a mobile wallet on the device of the sender or recipient and is exchanged and transacted through a deposit and withdrawal system that allows for debit and credit entries to be made in the account record of the respective parties. This is achieved through device software that is only available to subscribers. The software is provided through a SIM card[60] or via USSD technology and allows the use of a special short code that triggers access by the device to a menu provided by the transaction processor.[61] The processor allows for the exchange of instructions through the interface and receives and verifies instructions, checks the feasibility of the transaction, based on the record of balances held on the issuer's account and then effects the instruction through debits or credits in that account record and thereafter shows the new account balances.[62] The balances are confirmed by the system to the respective parties through an electronic message and settlement occurs, where money or value is delivered to the recipient, less any ensuing fees.[63]

Parties add value into the system at retail outlets by exchanging cash for credit in the system.[64] The retail outlets draw cash by paying it out to a party in exchange for credit in the system.[65] Access to the system by retail outlets is through the same interface and transactions that they complete will earn them a fee. They similarly maintain an account and transfer electronic value from that account to customers' accounts in exchange for cash received.[66] The overall pool of funds is maintained by the MNO at a banking institution.

The nature of the mobile money transaction is arguably a disincentive to misuse the system, as it

54 Chatain *et al. Protecting Mobile Money* 12.

55 *Ibid*.

56 Andiva "Mobile Financial Services and Regulation in Kenya" (2016) 3 https://static1.squarespace.com/static/52246331e4b0a46e5f1b8ce5/t/5534a332e4b078bae80cbaeb/1429513010529/Barnabas+Andiva_Mobile+Money+Kenya.pdf (accessed 21-02-2022).

57 Merritt "Mobile Money Transfer Services: The Next Phase in the Evolution of Person-to-Person Payments" (2011) 5(2) *Journal of Payments Strategy & Systems* 143, 147.

58 Chatain *et al*. *Protecting Mobile Money* 13.

59 *Ibid*.

60 *Ibid*.

61 *Ibid*.

62 *Ibid*.

63 Chatain *et al. Protecting Mobile Money* 13, 14.

64 *Ibid*. 14, 16.

65 *Ibid*.

66 *Ibid*. 16.

provides transactional traceability and makes it less of a threat from the AML/CFT perspective in instances where anonymity would be a key attraction for criminal elements.[67] However, funds may be moved without disclosing the purpose of the transaction, as the interface does not make such disclosure a precondition for the movement. It may be argued that correspondingly, normal banking transactions similarly do not verify any declared purposes. This is nonetheless an avenue that could be misused by criminal elements in a broad money laundering or terrorist financing scheme. Illegitimate purposes are unlikely to be disclosed or detected through the movement of funds in the system. The system also allows merchants and agents to receive and disburse funds and could facilitate intentional or unintentional laundering and terrorist financing activity, especially where the funds are received or disbursed with criminal intent. The storage and swift, real-time movement of value between subscribers and/or agents and the purchase of goods and services from merchants often concludes without directly involving a bank account or banking institution. With the heterogeneity of stakeholders, there is also unlikely to be common regulatory oversight, thus raising the prospect of criminal abuse and possibly money laundering and financing of terrorism.[68] In practice however, global standard-setting bodies encourage coordination and cooperation to prevent this prospect.

The advent of the COVID-19 pandemic resulted in a global shift to contactless and cashless payments. In jurisdictions where use of mobile money was already well developed, the regulators generally mandated higher daily transactional thresholds and suspended transactional costs to encourage the population to access and use this service as the preferred method of payment during the health crisis. In some instances, customer onboarding was made easier with account opening regulations eased.[69] As a result, there have been significant changes in the way consumers behave and digital channels have taken on greater importance.[70] Businesses are increasingly seeking to enhance their virtual presence by boosting their sales through digital channels and accepting more contactless payments. This is likely to persist even after the pandemic. The need to make pandemic social assistance payments also compelled governments to relax the rules with full consideration of the attendant risks of criminal abuse.[71]

The FATF has recognised this shift and whilst encouraging the adoption of new payment methods, acknowledges that criminals have been presented with "new opportunities to commit crimes and launder the proceeds" resulting in greater vulnerabilities occasioned by changing financial behaviour and the growing demand on institutions to detect any anomalies.[72] The growing economic effects of the pandemic could also increase the risk of exploitation of persons as money mules.[73] Remote working arrangements also put added pressure on compliance staff as they seek to work with the same pre-pandemic efficiency.[74] In the MFSs context, on account

67 *Ibid*. 16; Di Castri, Grossman and Sihin *Proportional Risk-Based AML/CFT Regimes for Mobile Money. A Framework for Assessing Risk Factors and Mitigation Measures* (2015) https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2015/10/Proportional-risk-based-AMLCFT-regimes-for-mobile-money.pdf (accessed 07-08-2019).

68 Zerzan "New Technologies, New Risks? Innovation and Countering the Financing of Terrorism" (2010) vii.

69 De Girancourt *et al. How the Covid-19 Crisis May Affect Electronic Payments in Africa* (2020) 8 https://www.mckinsey.com/~/media/mckinsey/industries/financial%20services/our%20insights/how%20the%20covid%2019%20crisis%20may%20affect%20electronic%20payments%20in%20africa/how-the-covid-19-crisis-may-affect-electronic%20payments-in-africa.pdf (accessed 11-09-2021).

70 De Girancourt *et al. Electronic Payments in Africa* 2.

71 Jenik, Kerse and De Koker *Rapid Account Opening in a Pandemic: How to Meet AML/CFT Rules for Social Assistance Payments* (2020).

72 FATF "Update: COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses" (2020) 5 https://www.fatf-gafi.org/media/fatf/content/images/Update-COVID-19-Related%20Money%20Laundering%20and%20Terrorist%20Financing%20Risks.pdf (accessed 13-09-2021).

73 FATF "Update: COVID-19-related" (2020) 18.

74 FATF "Update: COVID-19-related" (2020) 19.

of the fact that the services are linked to the network through a SIM card, control of the card then becomes more attractive for criminals and may be gained through SIM swap fraud.[75] This, coupled with the potential for money mules and the affordances of the MFSs ecosystem, makes the detection of money laundering activity and financing of terrorism even more complex. Money mules would be used in the placement process and, with the harsh economic times occasioned by the pandemic, the attraction to earn some extra money by cooperating with criminals in this placement process may become more attractive for an increasingly needy populace. As the acceptance of mobile money by businesses gradually grows, there is also potential for criminals to take over struggling businesses, create an illusion of higher turnover and launder money through them via the MFSs ecosystem.

The process of onboarding customers and the know-your-customer (KYC) requirements may potentially also be the subject of greater focus by criminals through the use of falsified identification to purchase multiple SIM cards, to give them access to mobile money accounts. There is an increased burden on entities that store personal information such as identity card numbers and dates of birth, to be especially vigilant as identity theft and crime may easily facilitate the creation of illegitimate mobile phone/money accounts if the information is accessed by criminals. With increased daily limits and no limit on the number of accounts an individual may have, there is the added challenge of monitoring this process to ensure that only legitimate subscribers are onboarded and that their transactions are legitimate. Whilst legitimate use of the increased limits is the norm, it is not unusual for law enforcement to make arrests and discover large numbers of SIM cards in the possession of criminals. Also, whilst there is still no evidence of this happening on scale, in the absence of an appropriate regulatory framework and effective monitoring, organised crime groups can easily exploit this mechanism and quickly transfer funds in small amounts even across borders from and/or to jurisdictions that may lag in this aspect.[76]

As a consequence of the increased risk and incidence of MFSs related criminal behaviour, policy makers, regulators and law enforcement agencies must adopt effective approaches to minimise the risk but, at the same time, to facilitate the adoption of these newer payment methods especially in the era of and after the current pandemic.[77] They must clearly understand the nature of the evolving risk and ensure that measures are taken to find a suitable alignment in their responses, with the overall AML/CFT objectives. [78]

3 2 MFSs – The Risk Factors

Insufficient information and knowledge of the existing and potential risk in the MFSs ecosystem could result in poor responses and ultimately, with every successful foray, increase the boldness with which criminals misuse the system. In the current pandemic era, where there has been a significant shift to newer payment methods, the potential for an increase in money laundering

75 The FATF reports an instance of an organised SIM swap scam the targeted dozens of victims and hacked their bank accounts. See FATF "Update: COVID-19-related" (2020) 26.

76 Allegations have been made against an agent in Kenya said to have registered 47 accounts in October 2018, using two handsets with different identity cards and names, out of 52 he registered in the last three months of 2018 and through which he is said to have received large amounts of money from South Africa and withdrawn the cash from a specific till at Diamond Trust Bank, before sending the funds to Somalia. See Faith Karanja, "Over Sh 100 Million Received by Terror Suspects, Court Heard Yesterday" *Standard Digital* (Online, 24 January 2019) https://www.standardmedia.co.ke/article/2001310546/terror-suspect-received-over-sh100m-months-to-attack (accessed 24-01-2019). See also Kakah, "Banks, M-Pesa Links in Dusit Hotel Attack" *Business Daily* (Online, 23 January 2019) https://www.businessdailyafrica.com/news/Banks--M-Pesa-links-in-Dusit-Hotel-attack/539546-4948276-77h3bx/index.html (accessed 24-01-2019).

77 Zerzan "New Technologies, New Risks?".

78 Di Castri, Grossman and Sihin *Proportional Risk-Based AML/CFT Regimes* 7.

and terrorism financing risk is also high where there is low-risk mitigation.

The typical mobile money transaction, particularly in the MNO-led model, allows a subscriber to receive, deposit and transfer money into a mobile wallet at will and to purchase goods and/or services without having to directly interact with a bank.[79] The speed and convenience with which this can be done, whilst a distinct feature and advantage of the system, is a risk factor, given that funds can be moved within and across borders, thus making it difficult for real-time detection and ought to be concerning to policy makers particularly in those jurisdictions that do not enforce strict and vibrant exchange control measures.[80] Every stage of the MFSs transaction has a potential vulnerability to the money laundering typologies.[81] As highlighted in the previous section, criminals may exploit the economic need occasioned by the pandemic to use money mules in the placement process. There is also potential to patiently open multiple accounts in multiple locations, with fictitious or stolen identification details and large scale, organised SIM swapping activity, to gain control of the related mobile wallets and extend the placement activity. The layering process would then benefit from the speed of movement of funds and the ability to withdraw cash from the system or to purchase goods for subsequent conversion into money. The ability of merchants and agents to receive and transact multiple payments daily, puts them in a unique position to enable the layering process, as they maintain their own records and have the capacity to deposit funds into any active account.

The main risk factors in MFSs have been identified as "anonymity, elusiveness, rapidity and poor oversight".[82] Anonymity relates to instances when subscribers are permitted to access services without registration and provision of identification documentation. Arguably, this would extend to instances where fraudulent identification has been provided or where the service is accessed by third parties, such as where devices are shared communally. Anonymity can also be associated with the ease of movement of funds within the MFSs ecosystem as there is generally no requirement to disclose the purpose of the transaction to enable or complete it and money can flow through the system without attracting the attention of law enforcement and compliance teams.[83]

Elusiveness refers to the practice of "mobile phone pooling", where multiple people access the service through a common device, or "mobile phone delegation", where subscribers permit other parties to use or manage the mobile device on their behalf.[84] This may occur where the registered subscriber is an entity and not a natural person or where device ownership is low and access to the service is shared by several related or unrelated parties. Ensuing transactions may not necessarily be attributable to the registered subscriber and may also not necessarily be with their consent and/or knowledge.[85]

Rapidity is a reference to the speed with which electronic value traverses the ecosystem. Value is available to a recipient instantaneously and can immediately be used to effect the range of transactions permitted by the system. This is clearly a risk factor that raises some concern about layering, especially in the context of organised crime and the use of multiple phones, by multiple people, in multiple jurisdictions and in quick succession.[86] With the linking of mobile

79 Mobile banking alternatives also allow for quick access to one's bank account and to transact much in the same way.

80 Vlcek 2011 *DPR* 416; Zerzan "New Technologies, New Risks?".

81 Solin and Zerzan *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks* 14–15 para 3.2.

82 Zerzan "New Technologies, New Risks?" 11; Chatain *et al. Protecting Mobile Money* 33–35.

83 Tongoi *Mobile Financial Services* 178.

84 Zerzan "New Technologies, New Risks?" 11; Chatain *et al. Protecting Mobile Money* 34.

85 Tongoi *Mobile Financial Services* 178.

86 *Ibid*.

wallets to bank accounts, it is also possible that subscribers could draw funds from a bank account remotely and deploy those funds into the layering process with relative ease.

Poor oversight results from inadequate regulation that fails to uniformly oversee the various MFSs players who are not all necessarily drawn from the same industry, or where there is regulatory arbitrage.[87] This challenge may be more pronounced with the work-from-home measures that resulted from the current pandemic and the difficulties this posed for regulatory compliance teams. It may also arise where there is outdated regulation and/or the absence of clear regulatory mandates between the different regulatory authorities mandated to oversee different parts of the ecosystem.[88]

Other factors may indicate potential money laundering or terrorist financing activity in the MFSs context. The sending of funds by one subscriber to multiple recipients or, where there are multiple senders to one recipient,[89] could potentially point to laundering or terrorism financing, even though sending to multiple recipients or receiving from multiple senders is not in itself wrongful. This is a concern in the context of "money muling" and what has become known as "digital value smurfing"[90] which involves multiple deposits of sums that are deliberately below reporting thresholds, by criminal recruits or under the direction of organised criminals, into mobile wallets to avoid detection by compliance and law enforcement teams.[91]

"High velocity or frequency of transactions"[92] could also potentially point to laundering or terrorist financing and would be evident from the speed and frequency with which the subscribers make or receive payments. A high frequency and volume of transactions could be indicative of criminal abuse, notwithstanding the fact that it is not in itself an indicator of any wrongdoing and is merely a "flag post" that calls for closer scrutiny[93] especially in an environment where the bulk of subscribers are considered to be occasional users of the payment service.[94]

The subscriber onboarding process generally requires the provision of an assortment of personal information prior to initial access to the service. Where such information is incomplete, or discovered to be falsified, there is need to more closely examine the subscriber account and the related activity.[95] Where the source of funds cannot be quickly verified or there are transaction patterns that suggest an attempt to defeat reporting thresholds or to convolute an audit trail, or where the transactions do not match the known financial capacity of a subscriber, there is a need to closely monitor the accounts for possible criminal abuse.[96] Multiple cross-border transactions which, by their very nature involve multiple currencies, may also be an indicator of potential criminal activity, especially where there is a high frequency. This is however complicated by growing multi directional diaspora remittances that may also have increased on account of the current pandemic and, further, that conventional acts of terror do not require large amounts of money.

87 Zerzan "New Technologies, New Risks?" 11; Chatain *et al. Protecting Mobile Money* 35–36.

88 Chatain *et al. Protecting Mobile Money* 36.

89 *Ibid*.

90 Cassara "Out of Africa: AML Compliance for Mobile Payments" para 14 https://www.mobilepaymentstoday.com/articles/out-of-africa-aml-compliance-for-mobile-payments/ (accessed 15-02-2018); Cassara "Mobile Payments, Smurfs and Emerging Threats" para 13 https://www.sas.com/en_us/insights/articles/risk-fraud/mobile-payments-smurfs-emerging-threats.html# (accessed 15-02-2018).

91 Tongoi *Mobile Financial Services* 179.

92 Chatain *et al. Protecting Mobile Money* 36.

93 Tongoi *Mobile Financial Services* 179.

94 Solin and Zerzan *Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks* 11 para 2.2.

95 Chatain *et al. Protecting Mobile Money* 36.

96 *Ibid.*

3 3 MFSs Risk Factor Measurement

The FATF, in its Report on New Payment Methods,[97] used a risk matrix that measured risk factors in relation to "risk mitigating laws, regulations, and industry rules and practices". It utilised identification, value limits, methods of funding, geographical and usage limits as the assessment criteria.[98] High risk was associated with methods that were characterised by:

i) anonymity in the accounts with no requirement for identification or verification;

ii) anonymity with no limits on their funding or transfers;

iii) anonymous sources of funds that were used to exchange value;

iv) cross-border payment methods and ease of access to cash.[99]

These risk factors, in an environment where mobile money has taken root, remain relevant in determining the level of risk. The more of these features that are identifiable in a payment method, the higher the likelihood of the risk of money laundering.[100] It is acknowledged by the FATF that every country has different risk factors with different ways of assessing that risk and therefore recommends the adoption of a "risk-based approach"[101] that enables the application of measures to prevent or mitigate money laundering or terrorist financing activity in a manner that is "commensurate with the risks identified".[102] This enables more efficient allocation of resources and the application of "enhanced" measures where higher risk situations warrant such measures and a higher allocation.[103] No method is prescribed by the FATF: each country must identify its own risk and create the necessary controls in response.[104] In the mobile money context, this requires an in-depth understanding of the functionality and design of the system and an appreciation of the potential for criminal abuse at each stage of the typical transaction so as to craft suitable controls.

4 INTERNATIONAL AML/CFT STANDARDS

4 1 The FATF Recommendations

The global AML/CFT regime is guided by conventions of the United Nations and the work of the FATF. The Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988); the International Convention for the Suppression of Financing of Terrorism (1999); the Convention against Transnational Organised Crime (2000); and the Convention on Corruption (2003),[105] which are ratified by Member States, are the relevant conventions. These are strengthened by the FATF which is mandated to develop and promote policies to safeguard the global financial system from money laundering, terrorism financing, and the financing

97 Financial Action Task Force "Report on New Payment Methods" (2006) http://www.fatf-gafi.org/media/fatf/documents/reports/Report%20on%20New%20Payment%20Methods.pdf (accessed 31-08-2019).

98 Financial Action Task Force "Report on New Payment Methods" (2006) 10.

99 *Ibid*.

100 Tongoi *Mobile Financial Services*180.

101 Financial Action Task Force "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations" 62.

102 *Ibid.* 9.

103 *Ibid.* 64.

104 Financial Action Task Force "International Standards on Combating Money Laundering" 6.

105 Jensen and Png "Implementation of the FATF 40+9 Recommendations: A Perspective from Developing Countries" 2011 *Journal of Money Laundering Control* 110, 111; United Nations Convention against Corruption, Treaty Series, vol. 2349, UN GAOR, UN Doc. A/58/422 (31 October 2003).

of proliferation of weapons of mass destruction.[106] It is in this context that the FATF made recommendations that present a "comprehensive and consistent framework of measures" to be implemented by countries in their financial systems to combat money laundering and financing of terrorism.[107] Each country is expected to customise the adoption of these recommendations and to ensure that the requisite standard is met. For purposes of ensuring compliance, each Member Country is subject to a review that assesses the level of implementation and identifies any deficiencies. Non-Member States are encouraged, through a coercive process, to implement the recommendations for purposes of uniformity in the global standard.[108]

The global benchmark for AML/CFT is the "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation" which comprises the FATF Recommendations, adopted in February 2012 and which have been endorsed by over 180 countries.[109] Under these recommendations each country "should criminalise money laundering on the basis of the Vienna Convention and the Palermo Convention" and "apply the crime of money laundering to all serious offences, with a view to including the widest range of predicate offences".[110] Each country must also "criminalise terrorist financing on the basis of the Terrorist Financing Convention" and "criminalise not only the financing of terrorist acts but also the financing of terrorist organisations and individual terrorists even in the absence of a link to a specific terrorist act or acts" and designate such offences "money laundering predicate offences".[111]

In February 2016, the FATF also adopted an updated Risk Based Approach Guidance for providers of Money or Value Transfer Services (MVTSs) which are defined as financial services that involve:

> the acceptance of cash, checks, other monetary instruments, or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer, or through a clearing network to which the MVTS provider belongs.[112]

This definition captures mobile money transfer services. In acknowledging the risk from new payment methods, the FATF has continued to highlight specific recommendations[113] as being of particular contextual relevance.[114] The following recommendations underscore the potential risk from new payment methods such as mobile money transfer services:

> i) Under Recommendation 1, countries must "identify, assess, and understand the money laundering and terrorist financing risks for the country" and "take action, including designating an authority or mechanism to coordinate actions to assess risks, and ap-

106 Financial Action Task Force "International Standards on Combating Money Laundering" 10.

107 *Ibid.* 6.

108 De Koker 2013 *WJLTA* 168; De Koker and Jentzsch "Financial Inclusion and Financial Integrity: Aligned Incentives?" (2013) *World Development* 267, 267; Finmark Trust "Anti-Money Laundering and Combating the Financing of Terrorism in Certain SADC Countries-Focus Note 1: Financial Inclusion and AML/CFT" 2015 http://www.finmark.org.za/wp-content/uploads/2016/01/FN_1_Fin_Inclusion_AMLCFT_SADC_2015.pdf (accessed 31-08-2019).

109 Financial Action Task Force "International Standards on Combating Money Laundering" 7. The FATF website however puts the number at over 200 jurisdictions. See https://www.fatf-gafi.org/countries/.

110 Recommendation 3.

111 Recommendation 5.

112 Financial Action Task Force, "Guidance for a Risk-Based Approach for Money or Value Transfer Services" (2016) 7 http://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-money-value-transfer-services.pdf (accessed 04-09-2021).

113 Financial Action Task Force "International Standards on Combating Money Laundering"

114 Financial Action Task Force "Guidance for a Risk-Based Approach" 12.

ply resources, aimed at ensuring the risks are mitigated effectively" and on that basis "apply a risk-based approach (RBA) to ensure that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified".[115]

ii) Under Recommendation 10, financial institutions are barred from "keeping anonymous accounts or accounts in obviously fictitious names" and are required to "undertake customer due diligence (CDD) measures" at inception of business relations, on occasional transacting, particularly when designated monetary thresholds are exceeded, where they suspect money laundering or terrorist financing activity, or where there is doubt about the "veracity or adequacy" of earlier data. The requirements involve "identification and verification of the customer's identity"; "identification of the beneficial owner"; "understanding the purpose of the business relationship"; and "on-going monitoring of the relationship".[116]

iii) Under Recommendation 14, countries must "take measures to ensure that natural or legal persons that provide MVTS are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations".[117]

iv) Under Recommendation 15, financial institutions must pay special attention to money laundering threats that come about from new technology that promotes anonymity and take preventative measures to curb this. Countries and financial institutions must "identify and assess" the potential money laundering and terrorist financing risks related to the development of new products, business practices, and delivery mechanisms and the use of new and developing technologies for new and pre-existing products.[118] The risk assessment must be completed prior to the launch of new product and appropriate management and mitigation measures put in place.

v) Under Recommendation 16, countries must "ensure that financial institutions include required and accurate originator information, and required beneficiary information, on wire transfers and related messages, and that the information remains with the wire transfer or related message throughout the payment chain".[119] They must monitor and take appropriate action in the absence of such information.

vi) Under Recommendation 26, countries must "ensure that financial institutions are subject to adequate regulation and supervision and are effectively implementing the FATF Recommendations".[120] They must also ensure that criminals do not acquire influential interests in the financial institutions. Service providers are also required to maintain and keep domestic and international transactional records and report any suspicious transactions to the financial intelligence unit.[121] These records include customer due diligence documents and identification documents which must be kept up to date.

vii) Under Recommendation 18, financial institutions must implement AML/CFT programmes and have internal policies, procedures, and controls, which include arrangements for compliance management and the screening of employees in the hiring process. They must also train their employees and have "an independent audit function to

115 Financial Action Task Force "International Standards on Combating Money Laundering" 10.

116 *Ibid.* 14.

117 *Ibid.* 17.

118 Financial Action Task Force "International Standards on Combating Money Laundering" 17.

119 *Ibid.* 17–18.

120 *Ibid.* 23.

121 *Ibid.* 15; Under recommendation 11 financial institutions are required to maintain records of all transactions for at least five years so that, if requested, they can provide evidence for the prosecution of criminal activity.

test the system".[122]

viii) Under Recommendation 20, financial institutions must make suspicious transaction reports to the financial intelligence unit (FIU), where they suspect or have "reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing".[123]

4 2 MFSs and the Difficulties in Implementing the Recommendations

The implementation of a risk-based approach allows institutions in any one country to assess their risk and determine their AML/CFT response. The assessment is largely dependent on an institution's understanding of risk and its interpretation of the measures that would meet the required standard. That assessment may sometimes result in the overestimation of risk by some institutions which may then resort to the application of enhanced due diligence measures, ultimately locking out perceived higher risk customers. For instance, in a study of compliance responses by banks in South Africa, their assessment of risk was found to be influenced by factors such as uncertainty about what the law requires and compliance obligations that may be overlapping or contradictory. Other drivers of conservative compliance behaviour included "institutional compliance culture"; industry approaches to compliance; business management processes; lack of expertise of compliance officers; "foreign compliance standards and requirements"; cost escalation concerns; management of requirements relating to discretion, where permitted; concerns relating to penalties and sanctions that may be incurred; amongst others.[124]

With increased global emphasis of contactless and remote payments such as mobile money and with the pandemic-related regulatory stances taken in a number of countries, to facilitate the uptake of the service by enhancing account balance and daily transaction limits and the relaxation of KYC requirements on subscriber onboarding, the emergence of higher risk must be contemplated. This would require enhanced monitoring to ensure that there is compliance with reporting obligations relating to suspicious transactions. The enhanced measures could result in financial exclusion through the locking out of high-risk customers, especially in instances where the risk has been overestimated.[125] Arguably the enhanced monitoring would entail more data analytics on more datasets. Financial exclusion is itself a risk that could push excluded customers to informal financial channels that pose a money laundering and terrorist financing threat. The reduction of financial exclusion is therefore important for the achievement of an effective AML/CFT system.[126] The temporary relaxation of the KYC requirements does not aid risk perception in the long run, especially where minimal or falsified identification information is collected in the onboarding process. On the other hand, overly rigorous due diligence may also be a barrier to the onboarding of persons who are unable to provide verifiable identification documents but are nonetheless potentially legitimate users. This would likely affect persons from remote and rural communities that do not have efficient access to government services and would have the effect of pushing them into informal financial channels, which do not necessarily cease to

122 Financial Action Task Force "International Standards on Combating Money Laundering" 18–19.

123 Financial Action Task Force "International Standards on Combating Money Laundering" 19.

124 De Koker and Symington "Conservative Corporate Compliance: Reflections on a Study of Compliance Responses by South African Banks" 2014 *Law Context: A Socio-Legal J* 228 229 233–247.

125 De Koker 2013 *WJLTA* 177; Malady, Buckley and Arner "Developing and Implementing AML/CFT Measures Using a Risk-Based Approach for New Payments Products and Services" 2014 https://ssrn.com/abstract=2456581 or http://dx.doi.org/10.2139/ssrn.2456581 (accessed 21-02-2022).

126 Di Castri, Grossman and Sihin 7.

exist on account of stronger formal payment channels.[127] Where identification documents have expiry dates, service providers may also take remedial action against customers and deny them a service that they have continued to access.[128]

The flexibility provided by this approach has the potential to result in the adoption of inflexible policy positions by institutions with respect to the assessment of risk and may in fact cause them to be more cautious and conservative in their approach to complying with the requirements.[129] With a more relaxed approach, as has been encouraged during the era of the pandemic, institutions could incorrectly interpret their level of risk and, with the regulatory uncertainty, open themselves up to compliance breaches that may prove to be financially and reputationally costly. The temptation to avoid the risk altogether could therefore raise the prospect of exclusion and the growth of informal channels and in fact, raise the country level risk.[130] There is, therefore, need for the provision of specific industry-related guidance on risk and related policy objectives, especially in the current era, coupled with an elaboration of their effect on compliance breaches.

Another difficulty that arises is directly related to the operational model adopted by the service providers in the MFSs context. Varying models allow for an MNO-led approach, where the only role that the banks have would be as custodians of the pool of funds in the account of the operator. In this model the MNO provides and manages the payment service, without the involvement of the banks and is therefore required to monitor the related AML/CFT risk right from the point of subscriber onboarding. MNOs ordinarily would be subject to oversight by a non-financial services sector regulator which may not be as adept in providing appropriate guidance on AML/CFT risk. Similarly, as MNOs are predominantly from the telecommunications industry, they may not have the same well-developed skills that the mainstream banks have in the identification and monitoring of AML/CFT risk. Where the model adopted allows for banks to take the lead, there may be similar regulatory inadequacy in that the relevant financial services regulators may be unfamiliar with the manner in which AML/CFT risk manifests in the MFSs ecosystem as a result of their primary focus being the regulation of the banking sector.[131] In either model, banks and MNOs must directly or indirectly collaborate for the efficient delivery of the service and there is a need for clarity on their respective responsibilities for, or onus of, AML/CFT compliance.[132] In the bank-led model, banking regulation would apply, placing the onus on the banks to lead the AML/CFT compliance process. In the MNO-led model the operator must take the lead.[133] This raises the need for an informed and appropriately skilled regulator that fully understands how risk manifests in the MFSs context.

Another difficulty that arises is the absence of a universally agreed definition of risk. The perspectives of institutions, regulators and policy makers may differ and therefore lead to distorted approaches to risk assessment and implementation of the recommendations.[134] Outcomes, as between the institutions themselves, or between the institutions and the policy makers, may vary significantly where institutions carry out their own risk assessment, especially where there is no national assessment of risk and, by extension, a definition of risk and what it constitutes.[135]

127 Malady, Buckley and Arner "Developing and Implementing AML/CFT Measures" 13; De Koker and Jentzsch *World Development* 277.

128 De Koker 2013 *WJLTA* 181–182.

129 Finmark Trust (2015) 6 para 5.2.

130 Finmark Trust (2015) 14.

131 Solin and Zerzan *Mobile Money* 4.

132 Chatain *et al. Protecting Mobile Money* 11, 114–115.

133 Solin and Zerzan *Mobile Money* 8.

134 De Koker 2013 *WJLTA* 183.

135 Tongoi *Mobile Financial Services* 188.

This is magnified by the diverse perceptions of risk and the related appetites for risk. Where, for instance, there are simplified customer due diligence provisions for lower risk customers, some institutions have nonetheless elected to maintain the application of "more comprehensive measures".[136] Various studies have shown that the fear of regulatory intervention may in fact cause some institutions to adopt a more conservative approach, even where there is an option to be less conservative, as may be seen from the way in which they treat identification requirements in the absence of national identity or residential address systems that could facilitate the KYC process. [137]

The risk perception will also vary depending on whether it is being assessed from a money laundering or terrorist financing perspective. The former may require monitoring of high-value transactions whilst the latter will be more focused on lower-value transactions, especially in the context of the newer types of acts of terror. What may appear to be low risk from a money laundering perspective, may in fact be high risk from a terrorist financing perspective. Simplified CDD measures would ideally apply where there is a low money laundering and terrorist financing risk.[138] Where the threat of terror is a real risk, it would not be tenable at all to employ simplified CDD measures, even if the perceived money laundering risk is lower.[139] The bulk of mobile money transactions are of lower value and could arguably be the subject of extended scrutiny, especially in countries that have had higher incidences of acts of terror. As the risk perception would depend on the institution's appetite and sensitivity, the end result could be a distortion of the assessment of that risk.[140] There is therefore a need to develop the capacity of institutions in the MFSs environment to create and execute AML/CFT programmes that enhance uniformity and certainty in the assessment and monitoring of risk in this context. In an age of multinational MNOs and an increase in cross-border and multi-jurisdictional transactions, differences and conflicts in legislation across these borders and, by extension, regulatory expectations, also add a degree of complexity in the approaches to assessment of risk.[141]

With renewed focus on the adoption of contactless payments and the potential for enhanced and creative criminal abuse, the role and autonomy of the FIU must also be scrutinised. FIUs have the potential to be misused or abused by the political class to protect their own, or to settle scores or gain some political advantage.[142] It is imperative that the FIU is impartial so that there is absolute clarity and certainty about its actions. It is also imperative that the FIU is suitably skilled and resourced and is able to provide informed and appropriate guidance on the assessment and evaluation of risk in each context. An under resourced and/or overly conservative regulator may pose a challenge to the effective implementation of the recommendations. [143]

In the context of cross-border and multi-jurisdictional transactions, the debate on harmonisation of money laundering and terrorist financing approaches must also be revisited. The considerable difficulty in achieving multi-jurisdictional uniformity may just make it increasingly possible for "forum shopping" by criminals seeking to operate without much scrutiny.[144] The FATF recognises that countries have "diverse legal, administrative and operational frameworks and

136 Finmark Trust (2015) 14.

137 Finmark Trust (2015) 14; Tongoi *Mobile Financial Services* 188.

138 De Koker 2013 *WJLTA* 185.

139 *Ibid*.

140 *Ibid*.

141 De Koker 2013 *WJLTA* 186.

142 Tongoi *Mobile Financial Services*189.

143 Conservative regulators who deal with conservative entities may have outcomes that overestimate risk. See Malady, Buckley and Arner "Developing and Implementing AML/CFT Measures" 10–11 16.

144 Finmark Trust (2015) 7.

different financial systems, and so cannot all take identical measures to counter these threats".[145] Each country will inevitably have different circumstances to contend with in the assessment of national and institutional risk and their approach will likely be different. The measures they take, upon assessment of risk, may not necessarily complement each other. Whilst this is an acknowledged fact, there is need to have a degree of cooperation between the different countries, despite any differences in their underlying policy, particularly because money laundering and terrorist financing activities transcend borders. Cooperation between countries would allow for decisive action to be taken even where the underlying activity is not a predicate offence in each of these countries. Harmonisation may not necessarily be the perfect remedy to all multi-jurisdictional AML/CFT difficulties, but it would certainly aid in progressing the global agenda of inclusion as countries develop a unique understanding of their respective challenges and find appropriate regulatory responses to them that bear some similarity.[146]

The mutational nature of money laundering and terrorist financing typologies makes the process of keeping technologically up to date that much more complex and costly. To be efficient and effective, institutions must maintain well-trained AML/CFT specialists and deploy state-of-the-art technology to ensure that they can consistently meet their compliance obligations and manage their AML/CFT risk. This can be costly and may frustrate AML/CFT efforts[147] in the MFSs context. To be effective, any AML framework must keep ahead of the criminals that seek to exploit the financial systems, through continuous state-of-the-art technology investment.[148] This could be financially burdensome and may, if passed on to subscribers, impact their service uptake decisions.

4 3 Potential Adjustment Areas

An enabling MFSs environment will allow greater access to financial services safely, conveniently and cost-effectively. Financial policy will traditionally enable regulation, supervision, and oversight to make financial systems and payment systems stable and efficient and to ensure consumer protection.[149] In contrast, AML/CFT policy, has traditionally focussed on the formal banking sector and seeks to safeguard the integrity of the financial system. This has conflicted with inclusion efforts which seek widespread access to financial services. Since AML/CFT policy is directed at risk reduction, any resultant increase of risk on account of stringent policy would have the opposite effect.[150] Achieving the right balance may also be challenging because policy makers are principally driven by a variety of factors[151] to "protect the financial system from risk" and AML/CFT risk is often also deemed to be an issue of national security that is subject to other more sensitive considerations.[152] There are some areas where the conflict may play out.

---

145 Financial Action Task Force "International Standards on Combating Money Laundering" 6.

146 Finmark Trust "Anti-Money Laundering and Combating the Financing of Terrorism in Certain SADC Countries-Focus Note 5: Harmonisation of regulatory frameworks in the SADC region"(2015) 17-18 http://www.finmark.org.za/wp-content/uploads/2015/08/FN_5_Harmonisation_-AMCFT_2015.pdf (accessed 31-08-2019).

147 Jaarsveld *Aspects of Money Laundering* 200 468.

148 Tongoi *Mobile Financial Services*190.

149 The International Monetary Fund defines financial policy in these terms. https://www.imf.org/external/np/mae/mft/sup/part1.htm#appendix_III (accessed 04-09-2021).

150 Collin *et al. Unintended Consequences of Anti–Money Laundering Policies for Poor Countries* (2015) 25.

151 See generally De Koker and Symington 2014 *Law Context: A Socio- Legal J* 228.

152 Barr, Gifford and Klein "Enhancing Anti-Money Laundering and Financial Access: Can New Technology Achieve Both?" (2018) 7 https://think-asia.org/bitstream/handle/11540/8277/es_20180413_fintech_access.pdf?sequence=1 (accessed 17-09-2018).

4 3 1 Customer Registration/Identification

To access mobile money services, the subscriber onboarding process requires the provision and verification of identification documentation. In the absence of such documentation subscribers may be barred from accessing the system or may only be allowed limited access. A policy that allows limited access to the service and therefore arguably enables more people to get connected, is more suited to the current pandemic era as it allows greater financial inclusion.[153] Studies have shown that where KYC procedures are complex, stringent or "burdensome" there is a negative impact on mobile money uptake.[154] The absence of identification documents may make the verification process less cost-effective for the MNOs and therefore discourage their engagement with the individual non-profitable subscriber. Identification documents that have expiry dates also place a burden of vigilance on the MNOs to ensure that such information is kept up to date. There is room to consider the use of a more dynamic method of identifying and verifying subscribers, particularly in an environment where access to the service may not be dependent on face-to-face interaction with potential subscribers. The FATF recommendations give guidance on acceptable types of identification[155] and have in fact highlighted the need to consider "digital identity, as appropriate, to aid financial transactions while managing ML/TF risks during this crisis".[156] In the post pandemic era, "digitized and digital" forms of identification must be seriously contemplated for purposes of customer onboarding and for the development and use of electronic KYC infrastructure to facilitate customer registration and identification.[157] This potentially allows for greater access to formal, regulated financial services, which is important as a disincentive to money laundering and terrorist financing activities and provides some protection from "fraud, financial abuse and exploitation" because transactions are traceable and enable the detection, investigation and reporting of suspicious transactions.[158]

4 3 2 Transaction Limits and the Risk-Based Approach

The enhancement of account balance and daily transaction limits, coupled with the speed and convenience of the transactions, arguably increases the attractiveness of MFSs for both legitimate and illegitimate users. Increased criminal abuse could adversely affect confidence in the payment system and highlights the need to have in place measures that safeguard the integrity of the system. The objective of the risk-based approach is to allow the deployment of more resources where there is higher risk and to be less stringent with the lower risk situations. Depending on the circumstances and the appetite and/or urgency of the launders, low-value transactions are less likely to be money laundering threats and may not necessitate the

153 Di Castri, Grossman and Sihin *Proportional Risk-Based AML/CFT* 16.

154 Di Castri *Mobile Money: Enabling Regulatory Solutions* (2013) 3–4 https://www.gsma.com/publicpolicy/wp-content/uploads/2013/02/GSMA2013_Report_Mobile-Money-EnablingRegulatorySolutions.pdf (accessed 13-09-2019); Lal and Sachdev "Mobile Money Services-Design and Development for Financial Inclusion" (2015) 15 https://www.hbs.edu/faculty/Publication%20Files/15-083_e7db671b-12b2-47e7-9692-31808ee92bf1.pdf (accessed 01-09-2019); Greenacre, Malady and Buckley "The Regulation of Mobile Money in Malawi" 2015 *Washington University Global Studies Law Review* 435 480.

155 The Basel Committee on Banking Supervision guidelines are more detailed in the nature of documents and data to be used in verifying identity of customers. See: Basel Committee on Banking Supervision: *Sound Management of Risks related to Money Laundering and Financing of Terrorism* (2014) https://www.bis.org/bcbs/publ/d505.pdf 34-44 (accessed 21-02-2022).

156 FATF "Statement by the FATF President: COVID-19 and Measures to Combat Illicit Financing".

157 Arner *et al.* "The Identity Challenge in Finance: From Analogue Identity to Digitized Identification to Digital KYC Utilities" 2019 *European Business Organization Law Review* 55 62–63.

158 Financial Action Task Force "Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion: With a Supplement on Customer Due Diligence" (2017) 2 http://www.fatf-gafi.org/media/fatf/content/images/Updated-2017-FATF-2013-Guidance.pdf (accessed 31-08-2019).

deployment of more resources.[159] Low-value transactions will, however, pose a similar threat to high-value transactions from the terrorist financing perspective, given that conventional acts of terror need not involve large sums of money or be drawn from illegitimate sources.[160] Matters of compliance may therefore become "conjectural" where the institutions are more inclined to avoid sanction for compliance breaches than to develop a responsive and effective approach to their assessment of risk.[161] Imposing transaction limits provides a useful avenue to address the potential integrity risk.[162] This approach has been used by a number of countries and involves the setting of limits on the amounts or frequency of MFSs transactions that each subscriber would be permitted to complete in a given period and may be through daily and/or monthly limits. Account balance and daily transaction limits will be ineffective if there is no corresponding limit on the number of accounts that one subscriber may have and transact.[163] The higher such limits are, the more attractive this payment system becomes to both legitimate and illegitimate users.[164] The low-value transactions however still remain attractive in the context of financing terrorism. Allowing a subscriber to maintain several mobile money accounts and to simultaneously transact on each at the threshold level, circumvents the entire concept of threshold limits. SIM card registration is a useful tool in tracking the ownership[165] of and usage of mobile money accounts as they are linked to particular cards and could therefore be an increasingly important avenue for addressing these threshold limits. There is a need to limit subscribers to a single threshold regardless of the number of accounts that they hold.[166] This would address a significant integrity gap. The system would need to be closely monitored for subscribers who have multiple accounts which may be used to circumvent account balance and transaction limits.

4 3 3 Use of Agents

The typical MFSs ecosystem, in jurisdictions where there has been success, involves a wide network of agents to enable greater access to the service. The agent networks consist of "regular retailers, post offices, supermarkets and/or selected agents" who can all "complete deposits, withdrawals, customer registration, identity verification and due diligence".[167] The FATF guidance envisages the delegation of specific functions to these agents. This approach presents an AML/CFT challenge in that the agents are not all drawn from the same sector and may be subject to supervision by a variety of regulators, which complicates the monitoring process to ensure compliance with regulatory obligations such as identity verification and suspicious transaction reporting. There is a need to have a robust system of compliance monitoring that ensures that each of the agents is properly screened, has received appropriate training, and has

159 See De Koker "Identifying and Managing Low Money Laundering Risk: Perspectives on FATF's Risk-based Guidance" 2009 *Journal of Financial Crime* 334 343–345 https://dro.deakin.edu.au/view/DU:30020721.

160 De Koker "Aligning Anti-money Laundering, Combating of Financing of Terror and Financial Inclusion: Questions to Consider when FATF Standards are Clarified" 2011 *Journal of Financial Crime* 361 371 https://dro.deakin.edu.au/view/DU:30039929 (accessed 21-02-2022).

161 Tongoi *Mobile Financial Services*193.

162 Financial Action Task Force "Money Laundering Using New Payment Methods" (2010) 26 https://www.fatf-gafi.org/media/fatf/documents/reports/ML%20using%20New%20Payment%20Methods.pdf (accessed 10-10-2021).

163 Financial Action Task Force "Money Laundering Using New Payment Methods" (2010) 26 para 77.

164 Financial Action Task Force "Money Laundering Using New Payment Methods" (2010) 26 para 78; See Kakah "Banks, M-Pesa Links in Dusit Hotel Attack" para 4–5 https://www.businessdailyafrica.com/news/Banks--M-Pesa-links-in-Dusit-Hotel-attack/539546-4948276-77h3bx/index.html (accessed 11-10-2021).

165 De Koker "Will RICA's Customer Identification Data Meet Anti-money Laundering Requirements and Facilitate the Development of Transformational Mobile Banking on South Africa?" (2010) 4 5.

166 Tongoi *Mobile Financial Services* 194.

167 Tongoi *Mobile Financial Services* 194.

the capacity to meet the compliance requirements with strong sanctions for non-compliance. In addition, or in the alternative the relevant IT system must be so well-designed as to limit the functions of the agent so that the agent is a source for the funds deposit and withdrawal process but can do little to undermine the controls.

4 3 4 Other Relevant Considerations

The fear of black listing of countries through the coercive FATF mechanism may tempt some countries to blindly adopt the law and regulation of other countries by domesticating them in a tick box approach, without full consideration of the suitability of such regulation to their circumstances and may resort to "sporadic piecemeal amendments" as the need arises.[168] The political will to craft effective AML/CFT policy and legislation is important and may be impaired where the political class is itself potentially subject to AML investigation and enforcement action[169] and is therefore reluctant to appropriately legislate. This could manifest through the setting up of compliance institutions that are deliberately inadequately resourced to carry out their mandates, or through the creation of multiple agencies with unclear mandates which create conflict in reporting obligations and promote regulatory arbitrage.

5 CONCLUSION

This article has drawn on the standards set by the FATF and assessed the potential role of MFSs in money laundering and terrorist financing by outlining the related processes and demonstrating how mobile money could criminally be abused to further these nefarious activities. It highlighted the global AML/CFT standards that countries are required to meet and drew attention to the growing risk of criminal abuse of MFSs in an environment where global standards may not be uniformly applied. It identified obstacles that may limit the efficacy of a harmonised AML/CFT policy in jurisdictions where MFSs have taken form and evaluated some of the challenges faced in the MFSs environment in the process of contextually complying with the international approach to combating money laundering and financing of terrorism. The article concludes by highlighting specific areas that require adjustment to safeguard MFSs from criminal abuse in light of the adjustments made in the current pandemic era with specific focus on the customer registration process, transactional thresholds and the use of agents.

168 *Ibid*.

169 A former Cabinet Minister and former head of a parastatal organisation in Kenya have been at the centre of AML-related extradition proceedings for several years. See Abugre "Tax and Banking Havens that Landed Okemo and Gichuru in Money-Laundering Trouble" https://www.businessdailyafrica.com/analysis/How-Okemo-and-Gichuru-landed-in-money-laundering-trouble-/539548-1215130-dnjjng/index.html (accessed 11-10-2021).