Money Laundering and Terrorist Finance in Africa: An Old Phenomenon in the Age of Rapid Technological Change

Jean Langlois + Benedikt Barthelmess, London, 2019

Abstract
Money laundering and terrorist finance have long been a great challenge in African nations with serious social, political and economic implications. Whoever studies the recent developments in this field will moreover notice that recent innovations in the financial sector and beyond have, on the one hand, resulted in the rapid broadening of citizens’ access to financial services; on the other hand, non-cash financial services in the form of the Kenyan M-Pesa, for example, have grown ever more removed from the reach of financial supervisory authorities and financial crime units. This, of course, renders the detection of financial crime much harder and the pressure has been increasing on local authorities to catch up with recent trends. Fighting financial crime comes, however, at an increasing cost for both financial institutions and government authorities; therefore, it is imperative for them to invest in technological solutions to tackle to burden.
### Content

1. **Introduction** ........................................................................................................................................ 4
2. **The Scale and Impact of Money Laundering and Terrorist Finance on the African Continent** ................................................................................................................................. 8
   2.1 **Overview** ..................................................................................................................................... 8
   2.2 **Macroeconomic Implications** ...................................................................................................... 9
   2.3 **Socio-Political Implications** ........................................................................................................ 10
3. **Terrorist Finance in Africa** .................................................................................................................... 11
   3.1 **Illicit Sources** ............................................................................................................................... 11
       3.1.1 **Criminal activities** ............................................................................................................... 12
       3.1.2 **Kidnapping for Ransom** ....................................................................................................... 12
       3.1.3 **Livestock Raiding** ................................................................................................................ 12
       3.1.4 **Extortion** .............................................................................................................................. 12
   3.2 **Legal Sources** ................................................................................................................................ 12
       3.2.1 **Legitimate Commercial Activities** ....................................................................................... 13
       3.2.2 **Fundraising and Crowdfunding** .......................................................................................... 13
       3.2.3 **Charitable and other Non-Profit Organisations** .................................................................. 14
   3.3 **Examples of Terrorist Organizations’ Funding Structures** .............................................................. 15
       3.3.1 **Al Qaeda** ............................................................................................................................. 15
       3.3.2 **Islamic State (IS)** .................................................................................................................. 16
4. **Money Laundering in Africa** .................................................................................................................. 19
   4.1 **Definitions of Money Laundering** .................................................................................................. 19
   4.2 **Defining the ML Process** .............................................................................................................. 21
   4.3 **An Example of a Successful Large-Scale Money Laundering Operation: the Legal Mafia Business** ............................................................................................................................ 23
   4.4 **Recent Trends in Money Laundering and African Specificities** ...................................................... 30
5. **Financial Crime and the African Financial System(s)** ............................................................................ 32
   5.1 **Offshore Finance: the Nexus of Money Laundering Operations in Africa?** ................................. 32
       5.1.1 **What is an offshore financial center?** .................................................................................. 32
       5.1.2 **OFCs as Common denominator in ML?** .............................................................................. 38
       5.1.3 **Mauritius: Africa’s Offshore Haven** .................................................................................... 39
   5.2 **The Rise of New Payment Methods: Even Greater Opportunities for Financial Criminals?** .............. 40
       5.2.1 **Prepaid Cards** ..................................................................................................................... 40
5.2.2 Electronic Purses ................................................................. 44
5.2.3 Mobile Payment Services .................................................. 45
5.2.4 Internet-Based Payment Services ........................................ 46
5.2.5 Digital Precious Metals ..................................................... 48
6 Tools to Combat ML and TF ...................................................... 49
   6.1 Global Responses .................................................................. 49
      6.1.1 FATF and FATF-Style Regional Bodies in Africa ............. 49
      6.1.2 IMF ........................................................................ 50
      6.1.3 Other Global Initiatives ................................................ 51
6.2 Regional Cooperation on the African Continent ..................... 52
      6.2.1 Algiers Convention ...................................................... 52
      6.2.2 AU Plan on Terrorism .................................................. 52
      6.2.3 2005 Action Program on Crime and Security Issues .......... 53
6.3 Weaknesses of Financial Crime Prevention Initiatives ............ 53
      6.3.1 Weak AML/CFT Framework ........................................ 54
      6.3.2 Lack of Training .......................................................... 54
7 The Use of Technologies in the Fight against Financial Crime .... 62
   7.1 Technologies’ Role in Reducing ML/TF .............................. 62
   7.2 Financial Institutions’ Use of Technological Solutions .......... 63
      7.2.1 Profiling Technologies ................................................. 63
      7.2.2 Deep Learning Technologies ....................................... 64
   7.3 Reg- and Suptech: Regulators and Supervisors’ Engagement with
      Technologies ........................................................................ 64
      7.3.1 Regulatory Sandboxes ................................................ 64
      7.3.2 Data Analytics Tools ................................................... 66
      7.3.3 Challenges ................................................................... 67
   7.4 Other Government-Driven Technological Solution ............... 68
      7.4.1 Digital Identification .................................................... 68
      7.4.2 Improved Information Sharing ....................................... 68
   7.5 International Technological Collaboration ........................... 69
8 Conclusion .............................................................................. 70
9 Bibliography ............................................................................ 71
1 Introduction

In his book "The Dollars for Terror: The United States and Islam", Richard Labévière noted back in 1999 that the current situation of Islamic terrorism was the result of a policy led by the United States akin to the story of the sorcerer’s apprentice. This reflection, which only precedes the 9/11 attacks by two years, has become even more meaningful today. Since the Second World War, be it in Central America, Ireland, Iran, Afghanistan or Europe, the world’s major powers have cleverly maintained terrorism, but ultimately ended up as its victims today.

Even though the end of the Cold War marked the end of government support as the main source of financing, terrorism has continued to flourish. Although several isolated states in the post-Cold War era still fund training camps and bankroll entire terrorist movements, most of the movements that survived the 1990s had to find other sources of income, notably from criminal activities. A key source has become drug trafficking which, in many instances, largely compensated for the dried-up state-sponsored financial support.

A closer look at recent insurgent movements reveals that most of them have invested in some form of mafia business, be it the majority of the protagonists Lebanese civil war, the PKK in Turkey, the Tamil Tigers in Sri Lanka, the FARC in Colombia or the warlords in Sub-Saharan African (Sierra Leone and Casamance are just two examples). Such mafia-style terrorist systems have thus become increasingly prevalent over time and, in the case of the conflicts in Afghanistan and the post-Soviet republics of Central Asia and the Balkans, they have become increasingly sophisticated and even democratized.

Such systems almost by default entail the laundering of the proceeds from related activities and, consequently, the world could bear witness from the 1990s onward, how money laundering (ML) became the modus operandi of terrorist financing.

---

Central to this has been the dilution of legal and illegal funds to reduce traceability, similar to the ML carried out by organized crime. This has, however, led some to argue that a distinction is nonetheless necessary between organized crime-related ML and the “blackening” of money earmarked for terrorist activities despite significant overlaps. On the one hand, money laundering, which is an “intrinsic component of organized crime”\(^2\) consists of giving an appearance of legality to income from illegal activities. On the other hand, terrorist finance is an inverted process in which at times legal proceeds are channeled to a criminal end-user. This is especially the case if charitable or government funds are employed to finance terrorism.

The key element that sets apart organized crime-related ML from TF-related ML is the fundamental divergence of objectives between organized crime and terrorist organizations. While the main purpose of organized crime is the generation of profits, the entire economy of terrorism is centered on the fulfillment of an ideological goal. The latter was demonstrated by the scrupulous care the terrorists of the September 11 took in repatriating a few thousand dollars that remained on their accounts before killing themselves. The difference also becomes apparent when we look at the volumes where TF-related amounts can be quite small while organized crime tends to move around colossal amounts of money.

Given these essential differences one might legitimately wonder why the fight against ML and the TF are assimilated when it comes to enforcement. This is mainly a reflection of the fact that the purpose of the policies to combat ML and TF is essentially the same. In both cases, the power accumulated by criminal and terrorist organizations such as the Colombian cartels or Al-Qaeda constitutes an existential threat to the institutions of the state, which through traditional means of repression can no longer be contained. In this sense, the fight against ML and TF then becomes a means of fighting more effectively against criminal or terrorist organizations when they cannot be attacked head-on. Of course, there is also governments’ hope that the implementation of anti-money-laundering (AML) policies along with specific combating the financing of terrorism (CFT) related

measures, will further help with the prevention of terrorist acts by also drying up the funding of terrorism from illicit sources.

It is hence difficult to look at CFT policies without taking AML policies into account and vice-versa. This holds particularly true on the African continent, the part of the world that is possibly most impacted by terrorism – the Institute for Economics and Peace estimates that more than one third of the global economic cost of terrorism is born by Sub-Saharan African countries alone. Home to some of the world’s deadliest terrorist organizations, such as Boko Haram and Al Shabaab, it is also a region where the overlap between terrorist and organized crime is particularly extensive. Boko Haram’s activities, for instance, span from microfinance ventures to robbery and looting.

Considering that Africa has greatly benefitted from the FinTech revolution, authorities tasked with the combat against ML and TF are facing an unenviable dilemma. New payments technologies have resulted in a sharp increase in financial inclusion in many countries, but at the same time much of these technologies have often been removed from the traditional financial systems to varying degrees, thus escaping the scrutiny of supervisory authorities. The most obvious example is probably the rise of decentralized distributed ledger (‘Blockchain’) technologies. Despite posing such challenges, new technologies have also been a source of opportunity for supervisory authorities and financial crime units.

Much has been said and written about the opportunities and the dangers arising from new technologies even in the context of financial crime. However, to date, no comprehensive attempt has been made to put these different aspects into perspective, notably in the African context.

This work therefore endeavors to fill this gap by providing an overview of the state of ML and TF across the African continent in the light of recent technological change. The remainder of this work is therefore structured as follows. An initial overview of the scale and impact of ML and TF in African countries will be followed

---

3 The term AML/CFT, as adopted by the Financial Action Task Force, is used in this work, to refer to anti-money laundering and combating of terrorist financing measures.

by a detailed analysis of the phenomena of ML and TF. From this we turn to an analysis of the wider system in which financial criminals operate with a particular focus on technological developments. Once this has been fully laid out, the last part focuses on the AML/CFT measures that have been taken, their weaknesses and, ultimately, possible technological remedies.
2 The Scale and Impact of Money Laundering and Terrorist Finance on the African Continent

2.1 Overview

If we are to appreciate the impact of ML and TF on African countries, we still have to rely often on anecdotal evidence and incomplete country-level data. However, there is a widespread consensus that large parts of Africa are particularly vulnerable to terrorism.\(^5\) Nigeria and the Democratic Republic of Congo (DRC) both figure among the world’s ten countries that are most impacted by terrorism in terms of the number of deaths.\(^6\) In Nigeria, the most active terrorist organizations are the Fulani and Boko Haram, an Islamic State affiliate, and account for 78 percent of terror related incidents.\(^7\) The DRC has been most affected by the terrorist activities carried out by the Allied Democratic Forces (ADF), Democratic Front for the Liberation of Rwanda (FDLR) and Mayi Mayi groups.\(^8\) Similarly, East Africa has not been spared of terrorism, the country most affected being Somalia. In Somalia, it was the Al Qaida affiliate Al Shabaab that is responsible for the majority of terrorist incidents.

The economic impact of terrorism in Africa is considerable. The Institute for Economics and Peace estimates that the economic impact of terrorism in sub-Saharan Africa amounted to USD 12.17 billion in 2018 or 37 percent of the global impact of terrorism.\(^9\) The African countries that suffered from the biggest economic impact are Mali, Somalia and South Sudan where the cost of terrorism is estimated at 1.4 percent, 1.1 percent and 0.9 percent respectively.

When it comes to ML, the Basel AML Index lists Mozambique, Liberia, Kenya, Benin, Sierra Leone, Cape Verde, Nigeria, Zimbabwe, Tanzania and Cote d’Ivoire among

---


\(^7\) Ibid. p. 21.

\(^8\) Ibid. p. 28.

\(^9\) Ibid. p. 31.
the 20 countries in the world with the highest level of ML/TF risk.\textsuperscript{10} In other words, more than half of the 20 countries in the world that are most exposed to ML and TF are located in Africa. The US Department of State’s annual “International Narcotics Control Strategy Report” paints year after year a similarly bleak picture of the state of ML and TF in this part of the world. It lists Cabo Verde, Ghana, Kenya, Liberia, Mozambique, Nigeria, Senegal and Tanzania among the major ML jurisdictions in 2018.\textsuperscript{11} Nigeria, the continent’s largest economy, is notably classified as “a major drug transshipment point and a significant center for financial crime and cybercrime”.\textsuperscript{12}

\section*{2.2 Macroeconomic Implications}

Estimating the impact of ML and FT on a country’s economy is difficult considering that financial crime is largely unobservable. The only directly observable data are those on prosecution for international ML, but these figures are only indicative of a very small proportion of the actual ML activity. It is, however, possible to identify a number of channels through which it influences macroeconomic performance. Peter Quirk, then economist at the IMF, in a working paper\textsuperscript{13} tests for the effects of crime, as a proxy for ML responding to criminal motives, on measured GDP growth rates in 18 industrial countries. He finds that ML using crime as proxy is closely and positively related to the level of government consumption with a lag of about four years. His estimate of the magnitude of the overall macroeconomic impact of ML amounts to 0.1 percent reduction in annual GDP growth rates for each 10 percent rise in ML associated with crime. While this growth effect estimates includes all direct and indirect effects, Quirk notes that it cannot be equated with overall welfare effects since notably non-economic costs and benefits are excluded from measured GDP.

\textsuperscript{12} Ibid. p. 147.
2.3 Socio-Political Implications

Apart from the economic dimension of financial crime in African economies, it is important not to neglect the socio-political dimension. Financial crime, after all, is a serious catalyst for state corruption. Take the example of an African state whose government is corrupt. This means that the representatives of this government regularly receive bribes, the size of which depends on the types of services provided. Once the bribes have been paid, through the recipients need to find ways to reintroduce these illicit payments into the official financial system. The direct implication from this is that a corrupt state with a weak AML/CTF legislation and enforcement has little incentive to change this as far as its government is concerned. Such a state is therefore exposed to the proliferation of corruption within his country. Clearly, in this context, corruption is, more than just an economic ‘cancer’, but much rather a political ‘cancer’.
3 Terrorist Finance in Africa

“Money is always and everywhere the sinews of war: terrorists need vital funds to buy weapons, vehicles and arsenals. International action to counter terrorist financing is a bastion of peace and security in the world” – Michel Sapin, former French Minister of Finance

The attacks of January 11 and November 13, 2015, as well as all unsuccessful attempts during the years 2015 and 2016 in France reminded us of the threat that terrorism represents for the country and everyone’s security. These events highlighted the importance of controlling terrorist organizations and especially their financing. Many measures have been put in place since September 11, 2001, reinforcing the existing mechanisms since the 1990s, particularly through the particular observation of identified terrorist groups.

What are the methods of financing terrorism? Terrorist financing is usually enabled by two types of actors, namely states and private interest groups. Through these parties, terrorist groups can access a range of different sources of funds. A study by the FATF identifies the following main sources: drug trafficking, extortion, ransoms, theft, fraud, games of chance including online, counterfeiting, support of certain states, donations, income from legal activities. Funds are thus derived from completely legal as well as illegal sources.

3.1 Illicit Sources

Large swaths of the funding for international terrorism are sourced from illegal activities. The UN Security Council in its resolution from 28 September 2001, notes the “close links between international terrorism and transnational organized crime, illicit drug, money laundering, arms trafficking and the illegal transfer of nuclear, chemical, biological and other life-threatening materials”. The main illicit sources of financing terrorist organizations use in Africa are outlined in this section.

---

3.1.1 Criminal activities

The 2016 FATF-GIABA-GABAC report\textsuperscript{16} has also confirmed information that terrorist organisations in West and Central Africa engage in robbery and looting to finance themselves. In the case of Boko Haram, robbery and looting was one of the organisation’s main sources of funding when it first came into being. For other terrorist organisations.

3.1.2 Kidnapping for Ransom

Kidnappings are commonplace in a range of African countries if media reports are to be believed. Kidnapping for ransom has long been practiced by Al Qaeda affiliates and it appears that Boko Haram has more recently been engaged in kidnapping; however, there is little data available about the ransom payments.\textsuperscript{17}

3.1.3 Livestock Raiding

The raiding of locals’ livestock is a confirmed source of terrorist funding in several countries. Nigerian authorities have reported a direct link between large-scale cattle thefts in Northern Nigeria and Boko Haram.\textsuperscript{18}

3.1.4 Extortion

A FATF-GIABA-GABAC report\textsuperscript{19} notes that a traditional financing method for groups operating in West and Central Africa is to extort local populations under the threat of violence. Money is taken from both regular businesses as well as migrant and drug traffickers.

3.2 Legal Sources

International terrorism is legitimately financed by state funding, donations and voluntary contributions and notably the “zakat”, a compulsory alms paid by Muslims. The existence of quite legal sources of financing increases of course the difficulty of detection. Especially, if some states have such an important role in the

\textsuperscript{17} Ibid, pp. 17-18.
\textsuperscript{19} Ibid. p. 10.
financing of terrorism, this poses a main obstacles in the fight against the financing of terrorism. The main legal sources of funding for terrorist organizations active in African countries are outlined in the remainder of the section.

3.2.1 Legitimate Commercial Activities
Citing Nigerian authorities, the 2016 FATF-GIABA-GABAC report\(^\text{20}\) confirms that legitimate activities such as the sale of farming products have been a source of financing for Boko Haram. In addition, Boko Haram has reportedly build up micro finance scheme to for small and medium-sized companies, allowing it to recycle illicit funds and generate legal profits. Lastly, Boko Haram is also reported to have used frontmen for business activities and to have interest in slightly larger enterprises such as haulage and transportation businesses.

3.2.2 Fundraising and Crowdfunding
According to a 2015 FATF report,\(^\text{21}\) fundraising through social media has become increasingly common with “the widespread access to and anonymity of the internet and especially the rapid expansion of social media”. To this end social networks are used for the coordination of fundraising campaigns which have in the past garnered donations from thousands of individuals.

The same report also identifies organised crowdfunding techniques as an emerging TF risk. Crowdfunding websites allow businesses, organisations or individuals to raise donations or investments from multiple individuals. Crowdfunding can be abused and employed for illicit purposes when, for example, the true objective of the funding campaign is masked. Such crowdfunding campaigns may pretend to be pursuing humanitarian or charitable objectives, but funds might ultimately be used for TF purposes.

---


3.2.3 Charitable and other Non-Profit Organisations

Charities have certain characteristics that make some of them particularly vulnerable to exploitation for the financing of terrorism. They generally enjoy the confidence of the public and have access to significant resources, in many cases in the form of cash. In addition, many of these organisations have a transnational presence which provides them with the necessary infrastructure required for national and international transactions. In certain countries they are subject to only limited or no regulation at all (in terms of registration, accountability, transparency, financial audit etc.). Light-touch regulation also means that they are often easy to establish without any need for initial capital and background checks on employees).

In a lot of countries charities functions outside of the scrutiny and supervision of state authorities. It is therefore far from easy to shut them down completely even when they are under investigation and/or accused of financing terrorism. Several cases are particularly interesting since they are very famous Islamic charities: the Islamic Relief Organisation (IIRO) which is based in Jeddah (Saudi Arabia) is focused on religious, social and humanitarian programs but IIRO and some of its subsidiaries have been named in various reports dealing with the financing of terrorist operations.

In 2008 the US Treasury accused Al Haramain organisation (headquartered in Saudi Arabia) of financing the Al-Qaida network. Also, Aqeel Abdul Aziz Al Aqeel (founder of Al Haramain) and Al Haramain’s subsidiaries in other countries, were accused of providing financial and material support to Al-Qaida and other terrorist organisations such as Al Itihaad al Islamia, the Egyptian Islamic Jihad, Lashkar e Tayyiba and Jemaah Islamiya. In 2009 the Pakistani police published a report stating that Al Haramain had contributed approximately 15 million dollars to jihadist groups in Pakistan. Much of the cash went to the Tehrik e Taliban (TTP), which is known for the assassination of Benazir Bhutto.

Another charitable organisation raised public attention in 2002 when the US
government and the Sanctions Committee of the UN Security Council designated it as terrorist. This charity based in Kuwait and with delegations in Afghanistan and Pakistan is the Revival of Islamic Heritage Society (RIHS). The subsidiaries of RHIS have been closed down by their respective governments in Albania, Azerbaijan, Bangladesh, Bosnia, Cambodia and Russia. Among other charges, RIHS headquarter (Kuwait) have been accused of lending both logistical and financial supports to the Pakistani terrorist organisation linked to Al-Qaeda, Lashkar eTayyiba (LeT), that was involved in 2006 train attacks of Mumbai and at the 2001 attacks on the Indian parliament. RIHS is also accused of being a key source of cash that enabled Jamaat Mujahidin Bangladesh (JMB), a Bangladesh terrorist organisation, to coordinate the 2005 attack. Somalan followers of Al-Qaeda also said that they had received significant amounts of money from RIHS.

Charities and other non-profit organisations have also been extensively exploited in African countries by terrorist organisations. The FATF/GIABA/GABAC has reports from Niger and Cameroon where funds were raised via such organisation.22

3.3 Examples of Terrorist Organizations’ Funding Structures

A closer look at some of the most prominent terrorist organizations with links to African countries reveals the ease with which certain organizations can raise millions and sometimes even billions of US Dollars to finance their operations. Examples such as the Islamic State further highlight the difficulties governments face in their endeavor to curtail terrorists’ access to finance.

3.3.1 Al Qaeda

Al-Qaeda, which has affiliates in Africa, such as Al Shabaab, has always used charities for its own agenda. It has been able to infiltrate employees in diverse charities to divert the funds allowed for legitimate humanitarian programmes towards its activities. In addition, Al-Qaeda was able to create its own network of

charities as a cover. Some of these networks sprung from the Jihad against the Soviet occupation in Afghanistan in the 1980’s. Since its inception, Al-Qaeda used fundraising as a tool to finance its operations. Studies show that the main group of donors were in the Gulf area and mainly in Saudi Arabia. It is also now clear that, even though some of these donors knew very well where their money was going, others did not really know. A lot of the donors made their contributions through money collectors; other funds came from corrupt employees working in charitable organisations who used the Muslim principle of charity to raise money for Al-Qaeda especially during the holy month of Ramadan. Several fundraisers had access to imams in mosques and obtained parts of the zakat (mandatory almsgiving) to finance radical Islam. Al-Qaida’s fundraisers used legitimate charitable organisations but also front organisations. This hybridisation of fundraising methods and sources enabled Al-Qaida to build-up a large and resilient funding network in the Muslim world, as well as in the foreign Diasporas. This became clear after many of the original fundraisers, such as Khalid Sheikh Mohamed, a senior leader of Al-Qaeda, had been arrested.

3.3.2 Islamic State (IS)

The Financial Action Task Force "identified ISIL -related funding streams, including revenues derived from control of oil fields and related infrastructure, kidnapping for ransom, trade with the United States gold or other valuable items and economic resources for sale on international markets ". Indeed the IS has three main sources of funding making the "Financial War on Terrorism" difficult because it is extremely difficult to limit these resources. First of all the revenues generated by selling what they captured, ie the sale of oil to the locals, to the Syrian regime as well as to the black market. IS also exports unrefined oil (crude) to Turkey. Indeed, it has been reported that ISIS "has consolidated its grip on oil supplies in Turkey, Jordan and Iran". The Institute for Economics and Peace estimates that ISIS controls about a dozen refineries in Syria and Iraq that would generate an average of $ 1 to $ 3 million a day. Moreover, the IS continues to enrich itself with theft and corruption in the Iraqi oil sector. The second largest source of IS funding comes from foreign investment and private donations from Kuwait,
Jordan, Syria, and Saudi Arabia, although this share of revenue is gradually declining. According to the Institute for Economics and Peace, the third IS resource comes from various criminal activities including extortion, kidnappings and looting. A low estimate of this source of revenue would be more than $36 million a year just by kidnapping humanitarian workers and journalists. The extortion including taxes on the premises would generate more than 8 million dollars per month.

Let us take the example of June 2014 to illustrate another method of IS financing: the Central Bank of Mosul and other smaller banks have simply been robbed allowing the IS to be enriched by $400 million and gold bars. On average, the IS would generate about $1 million a day with its activities, which makes it one of the richest terrorist group on the planet but which especially does not reassure because of its long-term financial capacity is extremely important. Moreover unlike other terrorist organizations the majority of IS resources come directly from Iraq or Syria, so it is extremely difficult to put in place sanctions and monitor these financial flows from a distance. Moreover, the implantation of the IS in the local fabric ended up making it take control of the economy of this geographical area.

The question that arises is, of course, to what extent the "Financial War on terrorism" led by the Americans and the rest of the world is capable of limiting ISIS access to its sources of funding and the extent to which on the one hand can find these financing networks and reduce them? US and international strategies set up after the attacks of September 11, 2001 to fight al-Qaeda are inefficient because the IS uses its resources "as an instrument of statecraft". The IS has put in place an economic war by adopting a profit model to finance attacks on a global scale without any on-the-spot checks being possible (notably bank regulations or military forces intervene to take away their cash).

The only thing that can be done internationally is to block ISIS access to the international financial system. A legislative response may be the condemnation and this is what the UN Security Council did in 1999 and in 2014. In addition, FATF has made recommendations to states to limit IS funding opportunities, notably by calling on states to: criminalize the financing of terrorism "on the basis of the Terrorist Financing Convention and should not criminalize the financing of
terrorism acts of the financing of terrorist organizations and even terrorists in the absence of a link to a specific terrorist act or acts. Countries should ensure that such offenses are designated as "laundering predicate offenses". The FATF also advises to put in place financial sanctions as required by the resolutions of the UN Security Council and especially "review the adequacy of laws and regulations that relate to entities that can be abused for the financing of Terrorism". NGOs are particularly vulnerable and states must ensure that they are not diverted. All states must also put in place systems to prevent the IS from accessing the international financing system including audits of clients, banks and especially money transfers. The FATF also advised to "ensure that individual providing money or value transfer services are licensed and sanctioned for lack of compliance", as well as to set up statements of sums held in cash in and out as well as regarding the holders of "financial instruments. Some competent authorities are designated to investigate further the true origin and destination of funds and their intended use. Finally, the FATF calls for "each country (...) to ensure that it has an effective and efficient approach to the protection of the environment. or entities connected to such activity".

There is of course the possibility of sending on the spot agents to help the Kurdish and Iraqi forces to set up a system of intelligence to direct military actions against the IS. However, it is a choice discussed and above all each state must be able to fight against its capabilities against terrorism and its financing.
4 Money Laundering in Africa

“Profit is fundamental to the goals of most crime, and therefore criminals make great efforts to move illegally obtained money and other assets in order to convert, conceal or disguise the true nature and source of these funds.” – FATF

4.1 Definitions of Money Laundering

Money laundering can be defined in several different ways. In etymological terms, the term describes the act of concealing the source and ownership of funds from unlawful activities and their discreet re-injection into the legal economic cycle. The list of unlawful activities is long it and, of course, depends on the jurisdiction. The possibly most common examples are bribery, currency counterfeiting, drug trafficking, espionage, extortion, fraud, murder and kidnapping.

The Financial Action Task Force on Money Laundering (FATF), recognized as the international anti-money laundering standard-setting body, defines money laundering as the “processing of [...] criminal proceeds to disguise their illegal origin”, further noting that “This process is of critical importance, as it enables the criminal to enjoy these profits without jeopardising their source”. In its 40 Anti-Money Laundering Recommendations, the FATF specifically incorporates the technical and legal definition of money laundering provided by the Vienna and Palermo conventions and recommends extending the crime of money laundering to all serious offences.

Indeed, at an international level, three United Nations (UN) conventions have offered further underpinnings to what qualifies as ML. Most countries adhere to the United Nations Convention against Trafficking in Narcotic Drugs and Psychotropic Substances signed in 1988 in Vienna. This convention adds that

money laundering also implies “The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from an offence or offences established in accordance with subparagraph a) [narcotics-related offences] of this paragraph or from an act of participation in such offence or offences”26. The Vienna Convention limits the predicate offences (i.e. the criminal activity of which the illicit proceeds are laundered) to drug trafficking offences. Going by this convention, offences that are unrelated to drug trafficking, such as tax evasion, kidnapping and theft, were not defined as money laundering offenses under the Vienna Convention.

In subsequent years, the international community felt that the predicate offence of money laundering should be extended beyond the definition of the Vienna Convention to cover other serious crimes. What followed were the 2000 Palermo Convention against Transnational Organized Crime and the 2003 Merida Convention against Corruption. The Palermo convention’s article 6 calls upon all participating countries to criminalize the laundering of proceeds of crime and establish the following as criminal offences, when committed with the knowledge of the involvement of proceeds of crime:

- Conversion or transfer of property
- Concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property.

The article furthermore calls upon states to strive to expand money-laundering offenses to cover "the widest range of predicate offenses".27

The Merida Convention offers further elaborations on money laundering and integrates the proceeds of corruption and bribery into the framework. Its article 14 further calls for the implementation of domestic regulatory and supervisory regimes for banks and non-bank financial institutions to “deter and detect all forms of money-laundering”.28

It is also worth mentioning that, historically, the term money laundering was popularized in the 1920s in the United States, at the time of Prohibition. A common technique used by alcohol traffickers then was to invest in Laundromat businesses which allowed them to blend “dirty” money from the illegal sale of alcohol with money from the legitimate Laundromat business. This phenomenon gained further momentum in the 1970s with the increase in revenue streams from drug trafficking by large criminal organizations. In a more recent yet significant, development over the last twenty years, money laundering has gradually abandoned archaic national structures and has instead adopted more flexible, internationally oriented organizational structures. Money launderers now often rely on specialized managers and advisers and pursue sophisticated strategies managing costs, profits and investments in search of economic profitability.

4.2 Defining the ML Process

Conceptually speaking, ML is an age-old phenomenon, but ML methods are constantly changing. In this sense the modalities of ML resemble the modern financial system in that they are progressive, sophisticated and international. Moreover, the basic definitions of the process of ML is reasonably straightforward, but, at the same time, the notion of ML is not easy to grasp in practice. Indeed, the phenomenon of contemporary ML involves a complex web of financial and economic processes which often individual stakeholders do not fully understand. Yet none of this prevents us to lay out the basic functioning of ML processes. With its ultimate objective of making illegally-gained proceeds, or dirty money, appear legal, money laundering consists of three main steps. At the first stage, ill-gained proceeds need to be placed into the financial system, a process also referred to as ‘prewash’ or ‘placement’. This can be achieved, for instance, via direct cash deposits at complicit banks, a front company or the purchase of assets. Often large amounts are parceled up into smaller less conspicuous amounts. This is also the stage where it is easiest to detect ML.

At the second stage, in order to ensure that they cannot be traced, the funds are ‘layered’ or ‘washed’ in a succession of often complex financial transactions. The purpose thereof is to eliminate the link between the funds and their illicit origin.
Well known layering methods are the conversion of cash into monetary instruments (traveler’s cheques, letters of credit, promissory notes etc.). Such transactional activities may involve the use of accounts under false names, or on behalf of persons or entities operating for other beneficiaries. Different intermediaries tend to be used for such transactions, including legal professionals and accountants, as well as front companies. With the involvement of these different parties, a complex web of transactions across multiple accounts on behalf of multiple individuals and front companies can be created.

Past examples of ML schemes show that the transaction activity observed in accounts often involve larger-than-expected amounts in relation to an account holder’s expected activity profile. Furthermore, the documentation reviewed by AML authorities, such as loan agreements, guarantees, sales or purchase agreements or letters of credit, is often incoherent and faulty. If an account is held by a business, the business often has only recently been incorporated and registered with the local chamber of commerce and/or the commercial registry. In addition, in many cases, the parties to the transaction appear to be related or may even be one and the same person. Another trend identified by ML experts is the use of representative offices of foreign banks to dispose of income from criminal activities. In fact, representative offices can offer a significant advantage for money launderers. In some countries, but not all, these offices may accept deposits and then transfer the funds to their own accounts at a local bank without disclosing the identity of the depositors and beneficiaries.

At the third and final stage, funds are then reintroduced into completely legal economic activities – a step commonly referred to as ‘integration’ or ‘recycling’. The investment into such activities or assets then generates perfectly legitimate returns. This is different from the layering process also in that the detection of laundered funds is provided through informants.

Two general observations can also be made on current trends in money laundering. First, some traditional techniques remain the preferred instruments for hiding illicit proceeds. Second, in addition to traditional money-laundering
techniques, authorities have noticed developments in the financial sector that pose significant threats to the effectiveness of AML measures. Although money laundering processes can have very different degrees of complexity, funds subjected to this process all pass through the financial system at some point. This system is the one used by international crime, but the experts are increasingly aware that international terrorism does not work in the same way.

4.3 An Example of a Successful Large-Scale Money Laundering Operation: the Legal Mafia Business

The turnover of the mafia in Italy is estimated at 135 billion euros out of which 25 billion are linked to legal entrepreneurial activities, which shows its weight in the legal economy. However beyond the money income, the real challenge of the mafia is much more a search for political power. What makes its strength is its ability to adapt to any economic system as legal. Contrary to what one might think, the boundary between legal and illegal activity is not so clear and it becomes almost impossible to perceive the characteristics of mafia systems in our current economic models.

This section aims to analyze mafia infiltration in the legal economy. To this end, we will try to define the legal-mafia business. We will then try to analyze the infiltration mechanisms of the mafia in the legal sphere. It will be shown that, it is by circumventing the law that the mafia manages to impose itself in the legal sphere. A look at the waste industry and the Neapolitan mafia (Camorra) helps to further illustrate a mafia entry mechanism into the legal sphere.

Illegal or unlawful activities are defined as prohibited by law or by a regulatory provision as it is contrary to public order. For example, drug trafficking is an illegal activity in that it affects the physical and mental integrity of the person. In a purely economic context, there are two main categories: illicit activities of a productive nature (trafficking in drugs, organs, prostitution, weapons, counterfeiting,

cigarette smuggling and loans with usury rates) and illicit activities of a distributive nature (financial extortion, bribery, ransom payments, rackets, robberies, etc.). With regard to productive illicit activities, it has been historically recognized that their characterization as such may vary not only in time but in space (the classic example being the Prohibition in the 1920s US).

Some activities are lawful in that they do not contravene the law but it is the methods of practice that are illegal. Activities may be lawful but not declared by the taxpayer, they can allow for tax evasion and the employment of undeclared workers without respect of the norms of safety of hygiene, environmental and so on.

As a criminal association the mafia carries out a large number of these illicit activities but that does not exclude all the mafia economic activities. This is particularly reflected in the legal definition in the Italian Penal Code of the mafia-type association in Article 416 bis, which was strongly emphasized by Professor Napoli: “The association is of mafia type when those who are part of it use the force of intimidation of the associative link and the condition of subjection and omerta which derives from it to commit crimes, to acquire in a direct way or indirect management or at least control over economic activities, concessions, licenses, tenders and public services or to realize profits or advantages unfair to oneself or others, or with the aim of preventing or hindering free exercise of the vote or to provide votes for oneself or others during elections.”

This definition is more supportive of the effects of the Mafia on the legal economic sphere and on the political sphere rather than on criminal activity. The criterion of the activity does not seem to be sufficient and must be supplemented by a second criterion in order to grasp the importance of all the economic activities of the mafia. Unlike other criminal associations, the mafia regularly chooses to invest in legal / lawful acts. Nor are they occult activities belonging to the underground economy. These companies are registered with chambers of commerce. On the other hand, it often happens that part of the activity is not declared to the tax authorities. What will differentiate a mafia business in a legal economy from other companies is the affiliation to the criminal association of individuals who exercise the legal activity the essential criterion becomes the property. It comes down to
asking whether the owner of the business belongs to the mafia or not. It is a discriminating factor that has at least a formal interest. It makes it possible to distinguish within the legal economy, the mafia legal sphere: legal by its activity, mafia by the identity of the owners of the social capital of the company. Mafia infiltration into the legal sphere, although it mainly concerns traditionally mafia geographic areas (such as the region of Puglia, Calabria, Campania, or Sicily), also concerns regions that do not have the same traditions of crime as Veneto, Lombardy or Piedmont. Mafia investments legally include commercial activities such as shops, hotels, supermarkets and especially restaurants; but also service companies, import-export regardless of the type of product or anything related to the building sector such as construction sites and different building materials. It can also be financial investment activities, in the field of insurance or in real estate (activity representing the largest share of income in legal mafia activities).

Legal-mafia companies are inalienable companies because they operate on mutual property rights and the blur on their real value makes it possible to postpone potential buyers. Moreover mafia organizations to hold these companies in the long term do not hesitate to take more and more control of existing businesses and not created by mafia. A historical perspective of mafia activities shows that legal activities have long been the target of the mafia and that mafia infiltration into the legal economy is far from a recent phenomenon. As Catanzaro and Lupo remind us, the mafia has always had a role in the legal economy, and the leading roles played by the mafia members were linked to the protection and intermediation of activities that are close to the productive and legal sphere. It was initially an indirect position, agrarian feudalism in Sicily does not allow mafia to own land and exploit. However from 1812 with the abolition of feudalism and the transition to capitalism the members of the mafia will be able to seize land and control more directly the local economy. This phenomenon can also be seen in Russia with the collapse of the socialist system. Members of different mafias have seized the property rights of companies undergoing privatization.

The observation of this type of process has given rise to theories concerning the "redemption of the mafia by legal activities" but this is not quite the opposite. It
continues to occupy important positions in old trades. Cocaine for 'Ndrangheta and heroin for the Camorra but also to develop new sources of income in illegal business as Saviano has studied very well with the waste traffic in Campania. Judge Falcone clearly states that there is no redemption of the mafia by legal activities: "No, the fact that mafia illegally enriched - and his descendants more than him - entered the legal economic world, no does not illustrate the resorption and neutralization of the mafia in society. Not today nor tomorrow. Because we never stop being mafia. And so, to refer to the laws and to use the typical Costa Nostra violence, to keep a caste mentality, a sense of belonging to a privileged layer. (...) God knows if I have seen in my career, starvation become rich and great entrepreneurs. But none has abandoned either affiliation or mafia methods. Their children either. " Paradoxically legal-mafia companies circumvent the law to better infiltrate the legal economy. Mafia infiltration reshapes the legal economy and has a significant impact on the behavior of non-mafia entrepreneurs. As recalled by Rey "It often happens that financial flows of the legal mafia economy feed the legal economy or that a lawful mafia company in turn allows to finance illegal profits: a contractor at the head of legal activity and criminals may decide to reveal fictitious profits from the legal activity. If it facilitates the camouflage of illicit profits. Conversely, he may decide to work at a loss in legal activities if it favors illegal profits." From his early work Arlacchi highlights the symmetry between mafia entrepreneur and non-mafia. Thus in 1983 he identifies what he calls three "comparative advantages" for the mafia enterprise:

i. Competition, discouraged by bullying and violence. The legal-mafia company by its status can create around the market it wants to acquire a ‘protectionist policy’ by managing to discourage competition. The processes are multiple and can range from threat to homicide. In addition, there is a close relationship between large companies in southern Italy (thus operating in mafia territories) and mafia organizations which contributes to creating a true mafia capitalism. Indeed mafia always offers outsourcing services cheaper than any of its competitors. What drives the big companies to go to the Mafia are especially the insurance of a protection and the
guarantee of not seeing neither their equipment nor their employees attacked. By doing so, these companies contribute to the market being regulated only by the Mafia and the destruction of the latest semblance of a legal industrial system. Indeed, if the legal-mafia company does not obtain its advantage in a direct way it continues to gain market share by this outsourcing game completely opaque.

ii. Salaries are suppressed by the muzzling of trade unions and workers’ associations. The legal-mafia enterprise has no qualms about overriding the obligations of labor law, social law, and taxation and even fewer trade union rights. As the region of Campania is extremely affected by unemployment, the mafia can impose paltry wages. Compelling pressure is exerted on the employees with controls on their professional life as private discouraging them directly to complain. The mafia is therefore present in all production reports and its means of pressure on the staff allow it to increase its productivity. It is important to note that most employees of these companies have an interest in obeying the mafia leader or have been placed. Many of them are former prisoners or notorious offenders.

iii. Legal-mafia enterprises have a very high capacity for self-financing (and therefore financial resources) compared to companies of similar size. However, the financing of even "legal" mafia programs does not come exclusively from the profits of these companies, but from mafia investment and capital generated by illegal activities. It is also a means of laundering "dirty" money. The mafia activities are highly lucrative: drug trafficking, weapons, kidnapping for ransoms, The anti-mafia law passed in 1982 has strengthened the institutional barrier between the legal and illegal economy, but it is the process described above that contributed most to the rise of these mafia companies. Another element has also allowed this boom: mafia companies have easy access to bank credit quite legal and this through its network of relations of both customers, friends and members ...

Arlacchi speaks of the mafia entrepreneur as an entrepreneur at "Kalashnikov". The legal mafia company can thus empty the area around it, non-mafia agents having to face a competition too dangerous. This causes a
sterilization of entrepreneurial potential in the territories occupied by legal-mafia enterprises. This simply involves self-elimination of the company's economic expansion so as not to attract the attention of legal-mafia companies or simply the waiver of the exercise of an activity. Entrepreneurial migration is also a statistically observable fact. Non-mafia legal enterprises heading to territories where the mafia has no influence or not at all.

As shown by Fantó, the deterrent effect favors a phenomenon of "institutional isomorphism". Indeed agents who are not Mafiosi have adopted illegal behavior or the limit of the legality either to resist the pressure of legal-mafia companies or possibly to work with legal-mafia companies. Fantó proposes a typology of the six types of relations between the legal enterprises and the legal-mafia companies: i) The report of co-participation, (the legal enterprise ceases to be autonomous and is directed directly or indirectly by a legal-mafia company) ; (ii) the exchange ratio (the two types of enterprises agree to render each other service and maximize their respective profits); iii) The associative collaborative report on an investment or several investments in particular (both types of companies have business relationships); iv) The relationship of cohabitation, (the legal enterprise finds a way to coexist peacefully with the legal mafia business); v) The protection-extortion report, (legal enterprises must regularly pay a sum of money to guarantee a certain level of tranquility); vi) The conditioning report (here it is the packaging that is the objective because there are competing interests with the mafia law firm). These different types of behavior are important in order to legally qualify the actions of different entrepreneurs during Mafia trials. Obviously there will not be the same type of penalties for a contractor willingly and actively complicit with the mafia and a contractor conditioned by the mafia. Illustration of the methods of entering the legal sphere with the example of the waste market and the Neapolitan mafia (Camorra)

The waste treatment sector is a monopoly of the Camorra which has managed to obtain this position by very efficient methods. The Camorra keeps the same way of
functioning that its activity is illicit or "lawful". Concerning the public procurement sectors, the mafia organization is waiting for a client to launch a call for tender and do everything in its power to win it by "conforming on paper" to the specifications issued and the different conditions of the contract. To do this, the organization uses young traders (the 'stakeholders'), the latter operate as drug traffickers They are also from the most prestigious European management schools and are responsible for allocating different markets to the Mafia. The reason why companies choose the Camorra is very simple, under cover of "legal" companies, the latter offer prices so low that they defy all competition. It is impossible to beat their competitiveness and attractiveness. The mafia has indeed understood that to infiltrate the legal sphere the mere threat was not enough, it is necessary to offer very interesting economic opportunities and be the most competitive. In their system everyone is winners: bosses to see their waste leave quickly, at low cost and especially not be under their responsibility, the mafia to make profits and organize as she wishes without there have no rules even less environmental nor adversaries. Saviano states that “the cost of properly disposing toxic waste imposes prices ranging from 21 cents to 62 cents per kilo or fifteen years the population the same service to 9 or 10 cents / kilo”.30

How is the mafia able to offer such low prices and maximize profits? The circuit is again very simple. First of all, the mafia organization buys by putting pressure on the owners or expropriating land which is often agricultural. Thanks to its relations with the local government, the Camorra manages to obtain authorizations allowing it to convert these acquired land in landfills. With this landfill status, the land is supposed to be capable of storing waste but in reality the standards of the European Waste Paper are very far from being respected. The dangers to the environment are enormous and extremely toxic waste can be dumped without any precautions. This type of waste is extremely dangerous because it infiltrates the groundwater and pollutes the water by rendering the surrounding land unusable. Then the mafia buys the companies that are used to pick up waste and their employees and force them to dump waste collected mafia

landfills. It is almost impossible for the leaders of waste collection companies to resist the pressure of Camorra families. Finally, the Camorra has infiltrated most of the municipal councils, and through the merchants it pays in addition to bribes only to the people making the decisions. It is with all these elements (trash, pickup companies and pots of wine) that the mafia can recover all these markets. The Camorra then reserves the right to respect or not the commitments made during the calls for tenders insofar as the contracts have already been signed. In practice, in order to reduce costs, the waste centers are overflowed and others are rarely rebuilt. It even happens that some old landfills are resold in building land for inexpensive housing estates.

4.4 Recent Trends in Money Laundering and African Specificities

Although conventional money laundering methods are still commonplace, there has been no lack of innovation in how some criminals launder illicit proceeds. Several trends can be identified which, to some extent reflect broader trends, such as switch to mobile solutions for commercial transactions which, in 2017, stood at 31% of global digital commerce. Money launderers have increasingly been using new payment methods (NPMs), as reported by FATF and the Groupe d’Action Financiere (GAFI) in 2010. Further increases have been reported more recently by national authorities. According to the FATF-GAFI report, schemes were brought to the supranational body’s attention that involved the use of prepaid cards or internet payment systems. NPM’s benefit from “anonymity, high negotiability and utility of funds as well as global access to cash through ATMs”. At least in some African countries, this development has likely been much more pronounced, although there is a lack of concrete data. A range of countries have witnessed a rapid proliferation of mobile payment systems, the most notable example being the Kenyan M-Pesa. It has been argued

32 FATF (2010), Money Laundering Using New Payment Methods, FATF Report, October 2010, FATF/OECD.
that the use of such alternative payment systems has increased the risk of ML.\textsuperscript{34} Another trend has been the increased use of more complex commercial structures and trusts set up by professional services providers.\textsuperscript{35} The implications of all of this will be further explored in the next sections.


5 Financial Crime and the African Financial System(s)

“Illegal transactions or financial discrepancies can take place anywhere in the world. There is, however, a lower risk of detection in African countries because our compliance programmes are often not as robust as they should be and in some cases simply ineffective” – José Pedro de Morais, Governor of the Banco Nacional de Angola.

The previous sections offered an overview of the basic processes of money laundering and terrorist finance, as well as the large-scale, detrimental impact financial crime has had on African economies. From this it has become clear that the financial sector is a central conduit for this kind of criminal operations and its role can only be fully understood if we take into account its different components, notably the ecosystem of on- and offshore financial institutions and financial services providers that has emerged over the course of the last few decades in the wake of financial liberalization. In taking this approach, it becomes instantly apparent that, on the one hand, the financial sector has been growing together, but, on the other hand, it financial systems remain fractured. This seemingly contradictory characteristic of contemporary finance has ultimately allowed cross border financial crime to thrive.

5.1 Offshore Finance: the Nexus of Money Laundering Operations in Africa?

5.1.1 What is an offshore financial center?

In 2000, the then Financial Stability Forum’s (FSF) Working Group on Offshore Centres, the G7 agency in charge of “promoting financial stability, improving the functioning of markets and reducing systemic risk”, noted in a report back in 2000 that offshore financial centers (OFCs) “are not easily defined”, but “can be characterized as jurisdictions that attract a high level of non-resident activity”. The

---

36 Pedro de Morais, J. (2016), The fight against money laundering – an African perspective, opinion piece, 16/01/2016, Financial Times, webpage accessed on 02/12/2019: https://www.ft.com/content/c8184a87-0590-3aa9-b0af-2c6ba5f28c33

International Monetary Fund’s (IMF) Monetary and Exchange Affairs Department concurs with this most basic definition in a report published in the same year. The FSF report further notes that traditionally the term OFC implied some or all of the following elements:

- Low or no taxes on business or investment income;
- No withholding taxes;
- Light and flexible incorporation and licensing regimes;
- Light and flexible supervisory regimes;
- Flexible use of trusts and other special corporate vehicles;
- No need for financial institutions and/or corporate structures to have a physical presence;
- An inappropriately high level of client confidentiality based on impenetrable secrecy laws; and
- Unavailability of similar incentives to residents.

In somewhat more prosaic terms, an offshore financial centers (OFCs) is a country or territory where two separate legal and control regimes for companies and the financial sector coexist. One serves its residents, similar to those in other countries, and the other one its non-residents. The latter is stripped of a number of prudential rules and certain transparency aspects, provided that a company or financial institution’s activities are exercised “offshore”, i.e. outside the host country. In other words, the offshore company may not have to disclose its board of directors or guarantee a certain capital base. In addition, it may benefit from strictly enforced secrecy and anonymity laws.

There are between 40 and 70 offshore locations around the world depending on the definition we employ. Most of these locations are micro-states scattered across the globe that have found a way to attract foreign capital by allowing it to avoid strict rules of control in their home countries. The offshore system constitutes an alternative economic development route, as opposed to industrialization.

---

strategies, for example. Many of the OFCs are British Crown Dependencies, or former colonies, and “are generally protected by Western hegemons with major capital markets” and one can argue that especially the smaller states “have traded their sovereignty to facilitate mobility of capital”.39

These micro-states thus perfectly correspond to the logic of the “enclave” that we evoked in relation to the laws and financial provisions of their close environment. As Judge Jean de Maillard points out in his essay ‘The market makes its law: "offshore financial centers adapt their internal regulations to allow those to evade the laws of other states. These states, on the other hand, consider that they are not only taking advantage of the financial globalization desired by the richest states, which allows them to offer capital attractive financial regimes. "There was never an obligation for one country to enforce the tax laws of another country," said one day in response to these reproaches the Minister of Justice of one of the Caribbean islands. If it is true that offshore places (or financial havens) have a very long history (counters, free ports, legal and commercial enclaves exist since ancient times), it is also true that since the 1980s they have experienced a vertiginous development. Indeed, the globalization of the economy and the proliferation of rules and safeguards in Western countries have created a stalemate within the states: globalization, which they wanted and promoted, would allow their capital and their businesses to legally escape the rigors of their internal regimes. The banker was still there, just like the merchant.

But, of their activities, they preserved on the national soil only those which they wanted to maintain. How then to profit from this other part of the profits which exists out of the money that the taxpayer reluctant to declare and dissimulates in his wool stockings? Simply by creating a "beyond“ forwarder and virtual that whiten the activities deemed illegal at home. The offshore allows to domicile in the space of its choice the benefits of these activities (or "omissions“ to the fisc)

without the country-home activities themselves. It is in this logic that offshore places have multiplied, countries have flags of convenience, free ports or tax havens.

All these concepts overlap, and it is not uncommon for a financial haven to include all these features. The offshore center is a country or a territory (some countries have established offshore zones within their own territory as Labuan in Malaysia) which proposes much more flexible legislation or even a lack of legal framework for companies registered in the country, country but do not engage in any trade in the country. A tax haven is a country or territory where a favorable tax system is granted to non-residents, or which raises no taxes on corporate income, whether in respect of residents or non-residents. These tax advantages are generally supplemented by rules or practices that protect the non-resident from prosecution in the country where he resides, such as, for example, strong bank secrecy or refusal to cooperate in international investigations. in tax evasion.

These tax havens can be at the same time offshore centers, but this is not always the case. The flag of convenience is a similar concept adapted to the merchant marine that allows registration of a ship in a country that is not the place of its main home port, and thus benefit from local legislation (or the absence of binding legislation, for example on the working conditions of seafarers or security measures) and the taxation of the flag country. As for the free port, or the free zone, it is a portion of a territory, usually fenced to avoid traffic, where the imported goods are not subject to customs duties when they are intended to be exported. It allows the transit of duty-free goods in a territory, sometimes after having been the subject of an industrial process, such as in Mauritius, where textiles imported into the free port are transformed into clothing which is then re-exported without see penetrated the territory in the customs sense of the term. This is most often a port for obvious reasons, the most famous being the Franc Colon in Panama, because of the traffic that has been discovered, often related to drug trafficking.
All of these mechanisms have in common to allow companies and persons who settle there to escape the tax, customs or legal obligations to which these persons and companies or their property may be subject in their country of origin. It is for this reason that, apart from attractive tax regimes, these financial havens, in the words of the United Nations, generally offer a whole panoply of associated "services" making it possible to conceal the origin of the funds and the identity, beneficiary, and to protect against the legal actions of foreign states. In the inventory of offshore financial and legal services, we note, in particular: -the registration of international business companies and offshore banks trusts, trusts or foundations, mechanisms for the transfer of ownership of funds or property, most often purely fictitious; -the domiciliation agencies responsible for ensuring a fictitious presence of the economic entity; -the "economic citizenship", which allows an investor of capital above a certain amount to acquire the nationality - and therefore the protection - of the host country. ; - strict legislation on banking secrecy. To this is generally added a weak judicial cooperation to repel requests for investigations from abroad.

To this is generally added a weak judicial cooperation to repel requests for investigations from abroad. The mapping of the offshore paradox is interesting: originally tax havens were in the immediate vicinity of highly regulated countries, in Europe or on the American continent. But today, while money is not necessarily physically transported, and the interest of offshore financial centers is more virtual than real, this need is less immediate. Russian organized crime, with the help of Chinese criminal organizations (the Chinese triads), has "invested" virtually in some Pacific islands where offshore company sponsors have never set foot. Some offshore centers located in islands with national sovereignty have been established from Panamanian law firms and operate only from there. Even better, offshore centers completely established on a so-called drilling platform outside territorial waters (and thus not subject to the territoriality rules) or simply imaginary like the "Dominion of Melchisedech" or
the "United Kingdom of Atlantis" have seen the ephemeral day, the time to sell diplomatic passports to offshore companies.

But it would be unfair to consider that micro-states with an extra-territorial economic or financial status are the only ones responsible for this situation. Especially since almost all the most important financial institutions in the country with a "regulatory hypertrophy" - and sometimes their own state-owned enterprises - are present in offshore centers when they are not at the origin of their creation. A US law, the Foreign Sales Corporation Act, allows large companies to fictitiously offshore offshore to avoid paying taxes in the United States and thus be able to make better offers than in international public markets.

The fact that money of criminal origin also benefits from these "tax free" spaces is only the consequence. For a long time, moreover, the problem was considered secondary. Offshore "products", which at the end of the 1980s represented only a tiny minority of the world market, now account for more than 30% of financial packages. It was therefore obvious that the integration and integration of criminal funds, through the mix, found a very hospitable environment that radically transformed the role of offshore places in the history of money laundering. Dirty money was no longer limited to "hiding" or passing through offshore places, but from the outset mixed with investment capital. In this way, he participated in major projects in real estate, derivatives, financing large international projects and the bond market-where there are no restrictions on the sale of securities to non-residents.

Thus, the specified financial engineering became a tool not only for large corporations, pension funds or states, but also for organized crime that mingled with each other. Mafias are not the only ones involved. Take the example of North American bank Riggs, which specializes in pension funds and real estate. It has been investigated by the Justice Department and the US Federal Reserve for hosting multiple and opaque Saudi accounts that have already
been used by the two pirates of 11 September. During the investigations, the investigators stumbled upon the company off the coast of Althorp Investment domiciled in Equatorial Guinea and under the Chilean dictator Augusto Pinochet. was examined for allowing the dictator to hide millions of dollars from his country's justice and tax authorities. The case, which was very complex, involved a similar airline, that is to say, a civil company, an insurance company, Lloyd's, an accused of compensation, a part of the victims of the attempt on the twin sisters. For the federal money laundering laws, the Federal Reserve and the end of the prosecution; in exchange, the Riggs Bank agreed to pay $ 50 million to the US Treasury. In this example, there is no question of dictators, dictators, rogue businessmen, and the other on the formal and limpid economy. There is only one economy with its rules, its shortcomings and often its condescension. There is no more money and the opposition of clean money.

5.1.2 OFCs as Common denominator in ML?

Commenting on the role of OFCs, a now somewhat dated UN Office for Drug Control and Crime Prevention from 1998 stated the following: “the common denominator in money-laundering and a variety of financial crimes is the enabling machinery that has been created in the financial havens and offshore centres”\(^{40}\) This perception has little changed over the last 20 years; instead, large scale, disclosures of documents belonging to offshore financial services companies have further corroborated this. The Panama Papers and, more recently, Mauritius Papers, have provided precious insights into the workings of a number of OFCs. Such an environment “enables some entrepreneurs to avoid regulation, taxes, undermine governments, and weaken the citizen-state contract”. Furthermore, “the proceeds can also be used to recruit private armies, fund gangsters, prostitution, and narcotics and undermine social order”.\(^{41}\)


5.1.3 Mauritius: Africa’s Offshore Haven

A key offshore location for African countries is Mauritius, which, as the international affairs magazine Foreign Policy once noted, “has an international reputation built around extremely low taxes – a flat corporate tax rate of 15 percent and effective rate as low as zero to 3 percent for offshore companies – as well as high levels of financial secrecy”\(^{42}\). The island’s offshore industry is a key pillar of the domestic economy and comprised in 2015 more than 21,000 registered business entities with USD 660.2 billion in total assets (nearly 60 times the size of the country’s GDP).\(^ {43}\) This also makes it one of Africa’s largest financial centres.

In light of its status as OFC, one may be surprised to learn that Mauritius was one of the first countries in the region to develop an AML and CTF regime.\(^ {44}\) Nevertheless, a 2018 mutual evaluation report prepared by the Eastern and Southern Africa Anti-Money Laundering Group, identifies significant weaknesses, notably:

- Lack of shared understanding of the ML/TF risk facing the country
- No assessment of the vulnerabilities of the non-profit organisations sector in order to identify possible exposure TF risks
- Financial institutions’ compliance responsibilities relate almost wholly to management companies (MCs)\(^ {45}\), with the exception of banks, which results in concentration risk, resulting in potential conflicts of interest
- Low levels of suspicious transaction reporting from MCs
- Lack of a robust system to assess ML/TF risks in individual FIs
- Inadequate legal and regulatory framework vis-à-vis sanctions


\(^ {45}\) Domestic companies licensed and regulated by the Financial Services Commission to act as corporate service providers.
- Implementation of targeted financial sanctions against TF in terms of UNSCRs 1267 and 1373 and successor resolutions ineffective
- Legal framework in relation to beneficial ownership not comprehensive enough

5.2 The Rise of New Payment Methods: Even Greater Opportunities for Financial Criminals?

African citizens have been rapidly pickling up digital solutions for money transfers and other banking transactions, which has been driven by the skyrocketing of mobile telephony coupled with large scale financial exclusion. The GSM association, a global trade body representing mobile network operators, estimates the number of mobile phone subscribers to reach 725 million by 2020. The New Payment Methods (NPMs) associated with this ‘digital revolution’ have created new challenges in relation to AML/CTF. A 2006 FATF report on new payment methods distinguishes between prepaid cards, electronic purses, mobile payments, internet-based payment services and digital precious metals. These different methods are increasingly interconnected among each other as well as with conventional payment methods. All methods merit closer scrutiny in the African context, as FATF and other AML/CTF reports and guidelines have repeatedly emphasised the potential of abuse by criminals and terrorist financiers, also specifically in African countries.

5.2.1 Prepaid Cards

Prepaid cards have been in use since the 1990s and were introduced as an alternative to credit cards, which require banks to evaluate the cardholder’s creditworthiness, and debit cards, which are linked to a bank account.

---

The FATF\(^{50}\) distinguishes between prepaid cards that are issued for limited or multiple purposes. Limited purpose prepaid cards are also referred to as closed system or closed loop prepaid card, as they can be used for predefined purposes often with restrictions to specific points of sale or specific services. They can be reloadable and non-reloadable. Examples for popular closed system prepaid cards in Africa are gift cards, sports cards, youth cards, and internet use cards.

Multiple purpose prepaid cards are also known as open-system, or open loop prepaid cards and can be used for a wider range of purposes than closed system prepaid cards. Such cards are usually linked to card payment networks, such as MasterCard or Visa, which means that they can be used in a similar fashion as debit cards for purchases and cash withdrawals. For some prepaid cards it is necessary to have a depository account. Most cards are reloadable. Examples are payroll cards and cash cards for people without bank accounts, debit or credit cards.

Prepaid card transaction volumes have grown at much higher volumes than those of debit cards.\(^{51}\) The global prepaid card market is expected to reach $3.7 trillion by 2022, up from $2.9 trillion in 2016 according to market research by Edgar, Dunn & Company\(^{52}\). According to the same market research report, growth has been particularly steep in Africa and the Middle East with 178% growth between 2012 and 2017 in light of the predominance of cash, the populations’ limited access to cash, the rapidly growing use of mobile phones and a range of prepaid programmes driven by consumers, companies and governments.

Governments, international organisations and non-government organisations have been championing prepaid solutions to advance financial inclusions and provide subsidies and other forms of targeted financial assistance to certain population groups. South Africa and Nigeria even went one step further by combining national identity cards with prepaid products. Companies have been using prepaid solutions to pay employee salaries. Younger consumers have notably been using

---


prepaid products for online transactions and student cards. Consumers of all generations have been using prepaid solutions to receive remittances from abroad. Prepaid initiatives have been led by both banks and mobile networks. In Nigeria, South Africa and Rwanda, banks have introduced mainly Visa prepaid cards. Other countries, such as Kenya, Tanzania, Sudan and Liberia witnessed the rise of prepaid initiatives, notably the M-Pesa, Tigo Pesa, MTN Cash and MTN Money. Most of the prepaid cards are network-branded payment cards allowing transactions with any merchant or service provider that is part of the payment network, such as Visa or MasterCard.

The FATF developed an evaluation matrix to assess the risks associated with different NPMs. The key criteria considered are identification, value limits and methods of funding, geographical limits and usage limits, as outlined in the table below.

![Payment Method Risk Factors Table](chart.png)
With respect to open system prepaid cards, the main identification-related AML/CTF risk lies with cards that do not require adequate customer due diligence as part of the application process. An example for such a card would be cards that can be purchased in a supermarket. Such risks may be mitigated by account and transaction limits. Value limits are normally linked to the market segment prepaid cards are targeting and, again, the main risk depends on how much can be held on a card, how often and by how much it can be topped up and how much can be withdrawn at a time.

Out of the different methods of funding, any anonymous method, such as cash and money orders, pose potentially much higher risks.

Open system prepaid cards can usually be used for cash withdrawals through the cash machine network, which constitutes yet another ML/TF risk. Some mitigation comes from the fact that most machines require a pin if one is to withdraw cash; however, a pin may still convey insufficient information about the user, depending on the pin issuance process. Usage limits per se can act as a mitigant; however the FATF cautions that cards may still be used to withdraw cash at qualifying points of sale. Another FATF report, moreover, notes that prepaid cards “are replacing travellers’ cheques as a method of moving money offshore”. In more concrete terms this means that a prepaid card could be loaded domestically using cash and then taken offshore to a high-risk or transit country with no declaration requirement at the border crossing. The funds parked on the card could then be withdrawn at various offshore cash machines with limited risk of detection.

The risk profile for closed system prepaid cards is slightly different. Such cards are not subject to any identification and may be resold for cash, which could facilitate ML/TF. High value limits pose a risk if they can be resold and utilised to move funds abroad. The resale potential and the ML/TF risk are closely linked to the

---

geographic limits or, in other words, the resale potential of a closed system prepaid card. Unlike open system prepaid cards, closed system prepaid cards cannot be used to withdraw funds from cash machines.

5.2.2 Electronic Purses

Electronic purses, according to the FATF’s 2006 typologies report, “is value stored electronically in a device such as a card with and integrated circuit chip (called a smart or chip card)”. ‘E-purses’ distinguish themselves from payment cards in that they does not have a magnetic stripe to store account information; instead e-purses store funds on the device’s memory chip – in other words, “the user is literally carrying his funds with him on the card”. Consequently, value can be transferred without funds passing through an account at an intermediary.

Value is placed into electronic purses in one of three ways: preloading, loading at issuance or top-ups to an existing purse.

E-purses were developed as substitutes for cash. In African countries, their use is mostly limited to small-scale transactions for specific purposes, such as public transport. The main types according to the World Bank are:

- Tokens consisting of units with no monetary value; instead units are, for instance, equivalent to individual journeys
- Transport money consisting of units equivalent to money, the use of which is limited for passenger transport fares. This could include multiple modes such as park and ride.
- Transport and micro-purchases purses similar to transport money purses, but with an extension allowing for other small purposes.
- eCash is a purse containing electronic money with full monetary value that can be used at any sales point with an accepting device and is exchangeable for cash.

---

According to FATF,\textsuperscript{57} identification-related risks depend on whether an e-purse is linked to a bank account or not. Most e-purses have relatively low value limits since they are usually intended for small scale transactions. E-purse programs tend to be geographically very limited which makes them generally unattractive for cross-border transfers of funds.

5.2.3 Mobile Payment Services

Mobile payments in general describe payments effected using mobile phones and other wireless communication devices.

Mobile payments are used in relation to both traditional banking services and what the 2006 FATF report calls “new mobile payments”. The former involves the use of a wireless communication device as access device to initiate and authenticate transactions from traditional accounts or payment cards and can thus be considered an “extension of traditional payment methods”. The latter does not require an underlying bank or payment card account and it is instead the telecom operator who “typically acts as payment intermediary to authorize, clear, and settle the payment”.\textsuperscript{58} Mobile device users can either have certain transactions added to their telephone bill (post-paid) or hold funds in an account with the telecom operator to make payments (pre-paid). In this sense, pre-paid mobile payments accounts resemble prepaid cards or electronic purses. As previously mentioned, a popular prepaid mobile solutions in Africa is the Vodafone-backed M-Pesa which, on the African continent, is available in Kenya, Lesotho, Tanzania, DRC, Ghana, Mozambique and Egypt.\textsuperscript{59} Another example is Inova, a company providing mobile money services in West Africa, Inovapay. Inovapay operates in partnership with money transfer business Western Union, microfinance bank Caisses Populaires, mobile operator Orange, insurance company SONAR and cable TV company ISEC, partnerships which have been...

crucial for the company to gain a critical mass of transactions to sustain what is essentially a low margin business.  

Regarding the associated risks, FATF\textsuperscript{61} argues that mobile payment services that are linked to a bank account have risk profiles similar to traditional bank accounts. For those accounts provided by the mobile operator and where loans are extended, identification processes are believed to be similar to traditional bank accounts. A potential AML/CTF risk arises from the fact that frequently telecom operators are not subject to banking supervision and regulation. In this sense, the main risk resides in payment service offerings that are limited to prepaid accounts because providers, in the absence of a credit risk and possibly adequate regulation and supervision, may be less incentivized to conduct full identification exercises on clients.

5.2.4 Internet-Based Payment Services

Defining internet-based or online payment services is not always straightforward, as payment services’ different components are not standardized and hence there is a lack of data on such payment services. Categorization of internet-based payment providers is further hampered because payment services tend to be associated with a single provider.\textsuperscript{62}

FATF\textsuperscript{63} defines internet–based payment services as “(i) payment services that rely on a bank account and use the internet as a means of moving funds to or from a bank account; and (ii) payment services provided by non-bank institutions operating exclusively on the internet and that are only indirectly associated with a bank account.”

\textsuperscript{60} Kamara, Y. (2012). \textit{Inova: A home-grown mobile money service in West Africa}, case study, UNDP.
The report distinguishes between non-bank internet-based services providers that allow users to hold accounts with the payment service provider and others that only allow for the sending and receipt of individual payments in conjunction with a customer’s existing bank account or credit card.

In the former case, i.e. payment services with individual customer accounts, the service provider may pool customer funds in a single bank account that may be held in the name of the service provider at a bank.

A 2013 FATF report64 offers greater granularity with respect to the different business models of internet-based payment services. The services are referred to as digital wallets, digital currencies, virtual currencies, or electronic money.

Of particular note are virtual currencies. Similar to other parts of the world, Bitcoin is the leading virtual currency on the continent, but there have been tens of other virtual currency launches in recent years. Launches include government-issued currencies such as the Tunisian eDinar. In countries, such as Egypt, Ghana, Malawi, Mozambique, Nigeria, Zambia and Zimbabwe facing high rates of inflation and limited trust in local fiat currencies, virtual currencies have been emerging as an alternative. The fact that virtual currencies remain unregulated might have further spurred growth. In addition, virtual currency-based remittance services have been on the rise, examples being Abra in Malawi and Morocco, GeoPay in South Africa and BitMari in Zimbabwe65.

The FATF report also highlights that in cases where internet-based payment services operate independently from a bank account, such as PayPal, the payment service provider may not have to meet the same AML/CFT requirements as conventional banks. In terms of identification, internet payment systems may permit anonymous accounts. Some service providers accept cash and money orders or transfer from anonymous prepaid cards, which poses more elevated ML/TF

64 FATF (2013). Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013, FATF/OECD.
risks. Offshore internet payment systems are a further source of ML/TF risk if they facilitate illegal transactions and cross-border transfers.

Virtual currency payment products and services present are particular ML/TF risk since this technology allows for anonymous transfers internationally. A FATF report66 from 2015 notes, citing the US Secret Service, that criminals are looking for and finding virtual currencies that offer:

- anonymity for both users and transactions;
- the ability to move illicit proceeds from one country to another quickly;
- low volatility, which results in lower exchange risk;
- widespread adoption in the criminal underground;
- reliability.

The report further notes that terrorist organizations have been promoting the collection bitcoin donations. Also, instances of arms trade involving virtual currencies have been uncovered by law enforcement agencies. With regards to online payment systems such as PayPal, the report highlights that such systems have also been associated with a number of terrorism suspects,

5.2.5 Digital Precious Metals

Digital precious metals are an online value transfer system involving “the exchange of options or the right to purchase an amount of precious metals at a specific price”.67 These derivatives can be exchanged between account holders on a dedicated digital platform. Prices of the virtual precious metals are based on the current price of the actual metal on commodity exchanges. In terms of the transaction process, the FATF notes that the process can involve two different service provides:

- the digital precious metals dealer who maintains the accounts containing digital precious metals
- digital precious metals exchange service which can function as a broker for the digital precious metals bought or sold by the dealers

The decision over the accepted methods of payment and the extent they let digital precious metal brokers or dealers access their services reside with the service

---

provider. The ML/TF risk is thus closely tied to this. ML/TF vulnerability is potentially further enhanced by the few geographic restrictions providers face.

6 Tools to Combat ML and TF

6.1 Global Responses

With the growing internationalisation of the financial system, African nations would struggle to effectively combat a range of financial crimes occurring in their countries without extensive international cooperation. Therefore, several international initiatives have been launched in past years.

6.1.1 FATF and FATF-Style Regional Bodies in Africa

At an international level, the first major step to combat financial crime was taken in 1989 with the creation of the Financial Action Task Force (FATF). This inter-governmental body came into being at the G7 summit in Paris as the first internationally coordinated response to growing concerns vis-à-vis the rise of financial crime. FATF brings together the representatives of the G7 member states, the European Commission and seven other countries.

By the FATF’s own account, its objectives are the setting of standards and the advancement of the “effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system”.

FATF has developed a number of recommendations, subject to regular reviews and updates that are globally recognised as “the international standard and norms for combating money laundering and the financing of terrorism and proliferation of weapons of mass destruction”.

This task force is therefore a decision-making body that seeks to generate the political momentum necessary to reform, within each member country, the laws and regulations in relation to financial crime. The FATF monitors the progress

---

made by its members in the implementation of recommended measures, examines the effectiveness of adopted policy measures to combat ML and TF and encourages the adoption and implementation of appropriate ML/CFT measures. The Task Force’s mission is subject to review every five years.

On the African continent, there are three regional AML groups, commonly known as FATF-style Regional Bodies (FSRBs), which have observer status with the FATF. These include:

1. Middle East and North Africa Financial Action Task Force (MENAFATF)
2. Eastern & Southern Africa Anti-Money Laundering Group (ESAAMLG)
3. Central Africa Anti-Money Laundering Group (GABAC)
4. West Africa Money Laundering Group (GIABA)

The development and strengthening of such regional bodies plays a vital role in the ML/CFT prevention. The FSRBs have not only an advocacy but also a mobilization role. They can also provide mechanisms to monitor developments in the fight against ML and TF and to facilitate mutual evaluations.

6.1.2 IMF

The IMF contributes to international efforts in a number of important ways, in line with its core areas of expertise. As a quasi-universal, collaborative institution, the IMF is a natural platform for information sharing, common strategy development and the promotion of sound AML/CTF policies. In addition, the IMF has built up significant institutional knowledge through its financial sector assessment work, financial sector technical assistance and oversight of member countries’ economies. This knowledge is particularly useful when it comes to understanding the extent to which national authorities comply with anti-money laundering and anti-terrorist financing standards, as well as the development of programs to help address deficiencies in particular areas.

After 11 September 2001, the IMF further broadened and deepened its involvement in the global fight against ML and TF. For example, in March 2004, the institution’s board of directors decided that AML/CFT evaluations and related technical assistance would become an integral part of the IMF’s operations. Later...

---

on, the board decided to again expand the scope of the institution’s activities to cover the full scope of the FATF Recommendations.

At present, the IMF is mainly active in the following three areas in relation to AML/CFT:

i. Assessments: The institution’s evaluations of financial sector strengths and weaknesses of the financial sector, which are carried out under the Financial Sector Assessment Program (FSAP) and the Offshore Financial Markets Program, include an assessment of the AML / CFT regime.

ii. Technical Assistance: In collaboration with the World Bank, the IMF has sharply increased technical assistance to member countries to strengthen their legal, regulatory and financial frameworks in the context of AML/CFT.

iii. Policy Development: The IMF and the World Bank together identify and analyze international practices in implementing AML/CFT regimes as a basis for providing policy advice and technical assistance attention to remittances because of the macroeconomic importance of these operations, especially in poor and developing countries.

Almost 20 years after September 11, 2001, the IMF commands over a large library of publications covering AML and CFT, such as guides to AML/CFT issues, manuals for financial intelligence units and AML/CFT legislation. IMF staff, furthermore, prepared working papers on a wide range of other related topics.

6.1.3 Other Global Initiatives

Another global initiative worth mentioning is the Global Financial Integrity (GFI) think tank with the objective of helping countries in their fight against financial crime. GFI works closely with Western policymakers and at international fora such as the G20, OECD and the FATF. In addition, they have been advising less developed countries, including countries in Africa, “to improve financial transparency and fight illicit financial flows”.

---


6.2 Regional Cooperation on the African Continent

In addition to the global initiatives outlined above, several conventions and cooperation initiatives have been adopted by African States at continent-wide and regional levels.

6.2.1 Algiers Convention

In 1999, the Organization of African Unity (OAU, which later became the African Union) adopted a convention on the prevention and fight against terrorism, also known as the Algiers Convention.

6.2.2 AU Plan on Terrorism

In addition to the Algiers Convention, an action plan for the African Union (AU) high-level intergovernmental meeting on the prevention and fight against terrorism in Africa was adopted in 2002. The AU Plan on Terrorism defines specific areas of action. These include ten specific measures to prevent the financing of terrorism, including the following:

i. The drafting of national legislation to criminalize ML and TF;
ii. Establishment of a Financial Intelligence Unit (FIU) responsible for dealing with suspicious transactions reports;
iii. Staff training to combat and prevent ML;
iv. Cooperation with international financial institutions.

In 2004, the AU also adopted a protocol to the Algiers Convention. The latter concerns the commitment of the member countries to implement the provisions of the OAU Convention on Terrorism and, among other things, to identify, detect, confiscate, freeze or seize funds that were used or intended to be used to commit acts of terrorism. It also provides for the establishment of a mechanism for allocating seized funds to compensate victims of terrorism and their families. The African Peer Review Mechanism (APRM), an initiative of the New Partnership for Africa's Development (NEPAD) and self-monitoring mechanism, includes a focus on the evaluation of mechanisms for controlling corruption. Promoting the

---

implementation of banking and financial standards is another key objective of NEPAD.

The AU also adopted a Convention on Corruption in 2003, which, however, has not yet been ratified by enough member states to enter into force. This Convention calls for the criminalization of the use or dissimulation of the proceeds of corruption (Article 4) and the laundering of the proceeds of corruption (Article 6). It also establishes a framework for regional cooperation aimed at improving mutual legal assistance, including extradition, investigation, confiscation, seizure and repatriation of proceeds of corruption.

6.2.3 2005 Action Program on Crime and Security Issues

An action program on crime and security issues was adopted by African leaders of 47 States at the Africa Round Table, which was held in Abuja, Nigeria, in September 2005. One of the six clusters included in the 2006-2010 Program of Action focuses on organized crime, ML, corruption, trafficking and terrorism. With regard to the fight against ML and TF in particular, the action program identifies three priorities for action and in particular designates the African Development Bank (AfDB) as a possible key partner for these activities. These include:

i. The development of national laws and strategies in line with international standards

ii. Institutional capacity building, including the creation of financial intelligence for the implementation of national laws and strategies;

iii. Support and assistance for the establishment of effective and operational sub-regional organizations to combat money laundering.

In their application, these initiatives have led to the creation of appropriate structures across the states.

6.3 Weaknesses of Financial Crime Prevention Initiatives

Before pointing out the range of weaknesses in the financial crime prevention regime in African countries, it is worthwhile to dwell shortly on recent improvements. The first key observation is that almost all states on the African continent have institutions and laws in place to fight ML and TF. However, the will,
and, above all, an effective implementation is often lacking. The main weaknesses can be grouped under four main areas:

6.3.1 Weak AML/CFT Framework

At a global level, the framework for improving the fight against money laundering is constantly evolving. This is unsurprising and necessary, considering that money launderers and terrorists constantly adapt their schemes to new technological developments and changing legal environments. The fight against financial crime is hence becomes increasingly complex. This means that it is crucial for supervisory authorities and financial crime units to make constant improvements in response to evolving threats in the financial sector. With this in mind, the FATF created an international framework to facilitate the consultation and the exchange of information among authorities. However, Africa remains the part of the world about which the FATF has the least information. This goes so far that, judging by the data, one would not think that the continent is home to several major international centers for ML.

6.3.2 Lack of Training

There is still a dearth of AML/CFT specialists on the continent. Moreover, in the broader population there is very limited understanding of ML/TF and its implications. Local authorities tend to engage in little outreach vis-à-vis the population. The reason is that national financial information processing units, when they exist within African states, do not or do very little outreach to practitioners. This obviously affects the populations. To the extent that, if practitioners are not sufficiently trained on the different developments of the concept at the international level, they can not validly deal with the training of populations on this problem. For example, one of the roles of the Royal Canadian Mounted Police (RCMP) as part of the national anti-money laundering initiative is to educate the public. To this end, the RCMP has developed a prevention guide for small businesses and foreign exchange bureaus in Canada. This has been possible because RCMP officers themselves have been trained and sensitized to the perverse effects of money laundering. This type of training aimed at popularizing the concept is however not yet widespread in Africa. If we take for example the State of Ivory Coast. How many
times have we attended debates, even on the radio, on the concept of money laundering? How many newspapers do you devote to just one page or even their editorial to talk about this scourge? Yet, in the light of all that has been said in previous chapters, money laundering, with regard to Africa, is a serious threat to development projects and may have an impact on the socio-political stability of States. This is largely related, in our view, to the fact that these structures do not themselves have the fullness of information. Indeed, many anti-money laundering structures exist within our African states. However, they participate very little in FATF meetings and other training seminars for them. The result is that the FATF does not have sufficient information on financial crime in Africa. The fault is linked to an opaque system where anti-money laundering institutions have very few means. They are limited and therefore cannot properly implement all the necessary procedures for the proper conduct of their work. This state of affairs is often attributed to the economic situation of the countries.

23 The actual or potential players in the economic and financial market Developing Countries (DCs), Middle Income Countries (MCP), Highly Indebted Poor Countries (HIPCs), etc. However, if we consider the funds that we manage to mobilize in Africa each year to fight against certain pandemics such as AIDS, would it not be possible, with a real organization, to mobilize resources for the formation of our practitioners? V ‘Low political will to combat money laundering, crime financing and corruption in general The previous line of thinking about the failings of the African system to combat money laundering has paved the way for the point we are now addressing. The lack of resources and training of money laundering cells and other bodies sometimes indicates a lack of political will to combat money laundering, crime financing and corruption general. The fact is that African states have up to now been prime targets for money laundering because of their constant need for foreign investment; but also because of the flexibility of their legal and tax laws in money laundering. Moreover, endemic corruption and misappropriation of public funds, coupled with the fraud and tax evasion prevalent in most of our African states, corroborate our position. The implication of such actions is manifested in a lack
of interest at the highest level of state decision-making on money laundering issues. The main reason for such acts arises either from a lack of knowledge of the impact of money laundering or from the pursuit of profit: • Ignorance of the impacts of money laundering The international economic impacts of money laundering are known around the world. However, the "corrosive" effects on states and populations are still unknown or simply neglected, especially in our African countries.

Profit seeking It has turned out that embezzlement is a common currency in some African states. In addition, the level of remuneration of employees of public administrations and sometimes even private, promotes corruption. In this context, African countries for which corruption is one of the popular "habits" tend to set up facade institutions to fight against money laundering when in reality it is not. Indeed, African states that have laws against money laundering are appreciated by the supervisory authorities (FATF, IMF, BCEAO, etc ...) because they seem a priori determined to fight against money laundering, this phenomenon. This situation also makes foreign donors more willing to invest in such countries. Some African governments therefore tend to develop formal laws that they do not actually enforce. Others go further, by creating, in accordance with the enacted laws, structures (CENTIF, etc ...) to which they allocate human and financial resources very insufficient to carry out their mission. In these circumstances, these countries have developed anti-money laundering laws only to make a good impression on international institutions (Bretton Woods, etc.), but also to reassure foreign lenders to benefit, moreover, from the development aids and other investments which could ensue thereafter in their favor.

1 'Institutional capacities The above point makes it easy to introduce the one developed at this level. Indeed, the fight against money laundering is more than necessary in Africa. Each state must therefore be vigilant and especially rigorous in the face of this scourge whose actors are followers of corruption and other similar malpractices. Many African countries have therefore created
national financial information processing units (CENTIF) in recent years. However, the institutions set up if they exist not only in name, do not have all the means they need to carry out their respective missions. For example, Togo initiated a two-day workshop in Lomé to reflect on its anti-money laundering strategy on March 30, 2009. Although the Togolese authorities had created a few years ago, Central Office for the Suppression of Illicit Drug Trafficking and Laundering (OCRTIDB). The realization, in 2009, of this workshop of reflection on the strategy of fight against money laundering in Togo, thus comes to corroborate the fact that the previous policies of this State were only very superficial, or required a real need of cropping. This reframing has unfortunately occurred only in 2009 when the scourge of money laundering has been around for a long time. In addition, the establishment last January, the National Cell Processing Financial Information (CENTIF) of Togo is in line with our previous observation. It is clear, therefore, that the capacity of African institutions to combat money laundering remains very weak.

> Training and awareness Structured training and technical assistance programs are essential for the establishment of institutions that can consistently combat money laundering in Africa. African countries can thus increase their own means of struggle to the point of becoming effective partners in the anti-money laundering campaign of the international community. In the United States, for example, there are ILEA24. ILEAs have been organized and funded by the National Institute for the Fight Against Proliferation of Narcotics and Law Enforcement in the USA (INL). Their mission is to provide courses for middle-level police officers in various countries. This training includes internships on financial crimes and money laundering. Seminars on these issues have also been organized for senior police officers in some ILEAs. This formula has worked well in Asia, Central America, South America, Russia, and Central Europe. The first ILEA for Europe was established in Budapest and focuses mainly on the training of police and criminal justice services in Central Europe. A 24 International Law Enforcement Academies in English International Law Enforcement Academies ILEA for South-East Asia was inaugurated in March 1999 in Bangkok, and more than a thousand civil servants from 10 countries in
South-East Asia attended its courses. An ILEA for Southern Africa opened on 23 April 2001 in Gaborone, Botswana. The example of ILEAs is very suggestive of the opportunities available to African states to participate, or even to develop, themselves, relevant training plans for the different actors in their respective financial sectors. Moreover, Botswana, through its rapprochement with the INL to establish an ILEA since 2001, shows us the way forward. As such, we can propose a simple method to detect that an action could be money laundering, even without having previously received training on this concept. It comes down to five (5) key questions: 1. Do I know this client well? 2. Do I fully understand the operation that the client wants to perform? 3. Am I reluctant to do this? 4. Is the transaction justifiable given the client's profile? 5. Is this a common way of doing this kind of operation?

In our opinion, sensitizing the general African opinion, especially practitioners (bankers, insurance brokers, casino employees, etc ...), to answer these five essential questions before starting any financial transactions with a customer would be a major step towards the total popularization of the concept of money laundering on the African continent. To do this, countries could use their media (broadcasting, television, etc ...) but also advertising (billboards, placards or simple posters depending on the means) so that every citizen feels directly concerned by this phenomenon, which, must he reminded, is constantly changing. > The institutional and political will More and more "citizens of the world" are refusing the prospect of living on a planet where many human activities are, directly or indirectly, under the influence of transnational criminal organizations with virtually unlimited economic and financial capabilities. Some of the highest spiritual authorities have, moreover, worried about the gravity of the threat. Pope John Paul II has spoken on this theme on a number of occasions; Thus, in the apostolic exhortation made public during his visit to Mexico in January 1999, he solemnly called on the churches of the American continent to mobilize against the "recycling of money". Each country must therefore ensure that its police and regulatory authorities and judiciary
communicate with each other, exchange the most important information and coordinate their activities. However, it will be necessary to wait to be sure that the expression of the political will will not be reduced to the presentation of successive "catalogs" of good intentions. It appears that the general context is rather favorable to the development of the recycling of money of more or less dubious origin, in particular of criminal origin. At the same time, the struggle efforts remain very international than national. Because, even at the scale of Europe, "Why do you want that the leaders of this political Europe put of good will to remove these networks of dirty money which they used to establish their power? [...] They protect themselves; unfortunately, by protecting themselves, they protect many other things. When you coerce judicial co-operation on corruption, you impede it

en tous domaines; vous l'entravez sur les trafics de drogue, le proxénétisme, la mafia [...]"

In view of all these factors, the fight against money laundering seems unlikely to take place in satisfactory conditions. Political, social, economic and financial issues are essential. Political, national and international authorities should, therefore, do their utmost to prevent the appearance of irreparable imbalances.

Support from private and informal sector institutions
While it is true that the fight against money laundering must be elaborated and conducted rigorously by each State, the fact remains that this task is not solely a matter of public service. In fact, private and informal sector companies can be the object of attempts to money laundering. Because, the latter generally show "ignorance" voluntary >> 26. As an example of "voluntary ignorance", consider a car dealer who does business with a customer interested in buying a car car worth 10 million FCFA. The customer, who wants to pay cash, goes out of a sports bag the exact sum in cuts of 10,000 FCFA and 5,000 FCFA. This payment method is very unusual. He should therefore immediately awaken the seller's suspicions. And in such a case, the latter has the duty to ask for explanations. However, our dealer does not, for fear of compromising a quick sale and lose a tempting commission. But the people who close eyes on key indicators of
money laundering, risk, through their "ignorance voluntary ", to be directly involved in money launderers' trafficking. 25 Quoted in D. Robert, Justice or Chaos, Stock, 1996, p. 47. 26 Voluntarily ignorant persons who, in order to avoid dealing with reality, knowingly neglect to take the necessary measures in a situation where there is a matter for investigation.

Therefore, if the buyer of the vehicle happens to be involved in a money laundering case, the dealer may be incriminated for complicity. It is necessary to get business leaders from the private and informal sector, mainly in the financial services sector (microfinance institutions, savings and credit cooperatives, etc.), that they support the initiatives of the against money laundering and financial crime. This could be done through training workshops for them. The Ivory Coast seems to have started to exploit this track. Indeed, a workshop to raise awareness of businesses and professions on the importance of the fight against money laundering and the financing of terrorism was held in Abidjan from June 17 to 19, 2009. It was three days of workshop work whose theme was " Impact of the informal sector on the fight against money laundering and terrorist financing in the WAEMU zone ". The objective of this workshop was therefore clearly to convince non-professional actors to get involved more in the process of combating money laundering and financing terrorism, two scourges that threaten national economic systems today. Such initiatives are to be encouraged and perpetuated. Thus, each African state, start with the Ivory Coast, could appropriate this kind of workshop and realize them at less than once a year to different companies in the private and informal sector. The aim is that, in the long run, these companies will be made aware of the dangers they money laundering and the effects that negligence their phenomenon can lead to the economies of the countries where they reside. In this way, private and informal sector companies can push back their instincts of "profit at any cost" to block against any attempts to money laundering that they may face. >
International cooperation The fact is that, unfortunately, the African continent remains one of the areas for which the FATF has less information. Perhaps because the FATF has been a pioneer in this area, the last five years have seen a number of international agencies taking a closer look at money laundering. Nevertheless, for the campaign against the threat of money laundering to be coherent and effective, it is necessary to coordinate the activities of all these bodies and to ensure that everyone plays a clearly defined role. Because, it is undeniable that the anti-money laundering measures often force the money launderers to move towards sectors of the economy badly armed for deal with this problem. In such cases, the national system must be flexible enough to extend countermeasures to new areas of the country's economy. In addition, national governments must work with other jurisdictions to ensure that money launderers can no longer simply move their activities to places where money laundering is tolerated. African institutions already have FATF observer status. It's a good start. Nevertheless, cooperation needs to be even closer. It is therefore incumbent upon each of the structures set up in Africa to communicate regularly with the FATF on the results of their investigations or possibly on the difficulties they encounter in the implementation of their due diligence. In other words, countries should actively participate in all international and regional meetings to increase their knowledge of money laundering and cooperation in this area. Our third part allowed us to give a general overview of the level of the fight against money laundering in Africa. It is in this context, moreover, that we were interested in the particular case of an Ivorian bank in which we had to carry out a mission of review of the internal procedures of fight against the money laundering. At the end of our work, it appears that Africa is struggling to really start an effective fight against financial crime. We have therefore proposed some solutions that could help improve the current situation. They boil down to raising awareness of the general African opinion through training for practitioners, then to the mobilization of the public and private sectors, and finally to close collaboration between the states in the fight against terrorism. money laundering.
7 The Use of Technologies in the Fight against Financial Crime

“Spotting bad behaviour is not easy, particularly when it lurks within an ocean of legitimate activity” - Megan Butler, FCA

7.1 Technologies’ Role in Reducing ML/TF

Especially in the lesser developed parts of the African continent, contemporary consumers have greatly benefitted from technological progress in finance, notably in the payments sphere. Arguably the greatest achievement of new payments solution has been the sharp increase in people’s access to basic financial services. However, as it has been shown in the previous section, new technologies have also been an enabler of financial crime, the anonymity granted by virtual currencies or the more and more widespread use of prepaid cards being just one example.

While tighter regulation and supervision has been the way forward to tackling financial crime, technology has to play a role if we are “to detect and disrupt financial crime, and ultimately the criminals who seek to exploit the system”, as Megan Butler, Executive Director of Supervision at the British banking supervisor FCA, noted in a speech on the 23rd of October 2019.

One could argue that this is even more so the case in Africa’s less developed countries where banks and non-banking institutions find it much harder to bear to the costs that have come along with a mix of machine and manual processes employed to comply with new AML/CTF measures. The FCA notably estimates the collective resourcing cost across the whole finance industry to amount to well over $1 billion each year. Greater vigilance within the industry also translates into larger numbers of reports filed with national banking supervisory authorities (e.g.

---

75 Ibid.
76 Ibid.
Suspicious Activity Reports, “SARs”\textsuperscript{77}). As a consequence, authorities across the globe have been struggling to cope with the increased burden of carrying out investigations, which, again, require tremendous amounts of resources. A recent report\textsuperscript{78} by the AML Working Group of the RegTech for Regulators initiative provides a particularly alarming assessment of authorities’ readiness for recent technological change:

In general, the information technology (IT) systems currently employed by financial authorities to capture, store, and render data from financial service provides (FSPs) and other sources were not designed for the latest generation of digital products, platforms, and provides that rely on Big Data. As these continue to proliferate across and within financial sectors, the capacity of existing data architectures to fully absorb and digest the data that digital financial services (DFS) generate is steadily diminishing.

Cheaper, technology-based solutions are thus the way forward in those countries – solutions that tap into Artificial Intelligence (AI), robotics, natural language processing and machine learning.

The following section offers an outline of these new technological solutions along with a commentary on the extent to which these technologies have already found applications in Africa.

\section*{7.2 Financial Institutions’ Use of Technological Solutions}

\subsection*{7.2.1 Profiling Technologies}

Financial institutions tend to rely heavily on profiling technologies that attempt to model and simulate ML behaviour in order to capture suspicious transactions. Automated profiling solutions have been in use for many years now.

Existing automated AML systems rely heavily on existing structured databases that lack the ability to effectively and efficiently identify hidden and complex ML

\textsuperscript{77} See for example the guidance provided by the South African Financial Intelligence Centre: Financial Intelligence Centre (undated). Financial Intelligence Centre Guidance Note 4 on Suspicious Transaction Reporting.

\textsuperscript{78} R2A (undated). Financial Authorities in the Era of Data Abundance: RegTech for Regulators and SupTech Solutions, white paper, p. 3.
activities, as Han et al. note. They further note that this holds particularly true for ML activities with dynamic and time-varying features. As a result, systems tend to produce a high percentage of false positives, which then need to be investigated by humans in what are often lengthy and human resource-intensive processes.

7.2.2 Deep Learning Technologies

Han et al introduce a framework that employs deep learning-driven natural language processing (NLP) technologies to augment AML monitoring and investigation. What is in its essence a distributed framework uses NLP technology to analyse news and tweet sentiments, entity recognition, relation extraction, entity linking and link analysis on data sources.

7.3 Reg- and Suptech: Regulators and Supervisors’ Engagement with Technologies

Financial regulators and supervisors have now for some time been looking into advanced data collection and analytics tools that are collectively referred to as “regtech” and “suptech”. A 2019 FSI insight paper by the Bank for International Settlements identified significant scope in the fight against ML/FT where technological tools are already advanced. This scope comprises both authorities with financial intelligence functions and AML/CTF supervisory authorities.

7.3.1 Regulatory Sandboxes

Regulatory sandboxes have been an innovation environment promoted by several regulators to allow the FinTech industry to test their innovation and understand the impact of regulatory measures. The first such sandbox was launched by the

---


80 Ibid.

British FCA in 2015, but the idea quickly gained traction and now more than 50 authorities worldwide are toying with such sandboxes. A report by the UNSGSA FinTech Working Group distinguishes between product testing sandboxes and policy making sandboxes, although the lines between the two types are fluid. Product testing sandboxes allow firms to assess consumer uptake and commercial viability. Meanwhile policy testing sandboxes are more focused on evaluation regulations or policies in view of their potential impact on new technologies and business models. Notable advantages include the reduction of uncertainty and hence the cost of innovation for FinTech developers, while the authorities find themselves in a better position to engage in evidence-based policy-making. The FinTech Working Group report also emphasises regulatory sandboxes’ potential to advance financial inclusion.

There has, moreover, been some experimentation with multi-jurisdictional sandboxes. Such sandboxes seem particularly promising when it comes to ML/TF prevention, given their international dimension. An added benefit is that it potentially allows for economies of scale, bringing down individual African regulators’ cost. Yet the FinTech Working Group report also cautions that the initial cost of setting such a sandbox may be high in light of the challenges the development of a sandbox framework across multiple jurisdictions may pose.

Regulators in African country have only limited experience with this concept to date. South Africa’s South African Reserve Bank and the Financial Services Conduct Authority have reportedly announced the creation of an innovation hub along with a regulatory sandbox. Other African countries that have been experimenting with regulatory sandboxes are Mauritius, Sierra Leone and Mozambique.

---

82 FCA (2015). Regulatory Sandbox, 11/05/2015, webpage accessed on 01/12/2019: https://www.fca.org.uk/firms/regulatory-sandbox
84 Ibid. p. 28.
85 Ngwenya, G. (2019). SA shouldn’t miss opportunity to move the sandbox beyond fintech, news article, 21/06/2019, Tech Central, webpage accessed on
7.3.2 Data Analytics Tools

Data analytics tools at hand include machine learning, cloud computing, natural language processing, text mining, application programming interfaces (APIs), artificial intelligence and machine reading. As Coelho, De Simoni and Prenio\textsuperscript{87} note, such technologies can be used for the detection of networks of related transactions, identification of unusual behaviours and, more generally, to transform large amounts of structured and unstructured data for analytical purposes.

7.3.2.1 Evaluation of FI Compliance with AML/CFT Requirements

Supervisory authorities’ mandate to supervise and monitor financial institution entails assessments of governance, risk management, internal controls and processes and systems to prevent financial crime. Coelho, De Simoni and Prenio\textsuperscript{88} find that analytical tools have been developed to enhance the offsite assessment of the individual institutions’ risk profiles.

7.3.2.2 Risk Scoring of Supervised Entities

Coelho, De Simoni and Prenio\textsuperscript{89} further note that advanced data analytics may be used to assess the overall risk of supervised institutions. Analytics tools typically assign a rating to each supervised institution as of their likelihood of non-compliance with AML/CFT requirements. Components of the risk rating could be risk factors such as an institution’s compliance history or reporting behaviour. The different risk factors can be determined using methods such as principal component analysis or geospatial analysis.

7.3.2.3 Identification of Patterns and Trends

A telling example for size of the incoming data flows financial authorities receive are the 15,000 calls from consumers reporting on scams and fraud which the FCA


\textsuperscript{86} Wechsler, M., L. Perlman and N. Gurung (2018). \textit{The State of Regulatory Sandboxes in Developing Countries}, SSRN.


\textsuperscript{88} Ibid. p. 7.

\textsuperscript{89} Ibid. p. 8.
received in the 12 months up to October 2019. In order to cope with such information deluges, authorities can turn to NLP to process complaints interviews and establish data analytics platforms using data science, machine learning and artificial intelligence to cope with large numbers of data points.

As outlined by a R2A whitepaper\textsuperscript{90}, the Central Bank of Nigeria (CBN), alongside the Nigeria Inter-Bank Settlement System Plc and BFA consulting firm, has been working on the redesign its data infrastructure. The so-called “Data Stack” consists of a transactional data warehouse and dashboards that CBN and other stakeholders can access to analyse payments data. It is populated via Application Programming Interfaces (APIs) with real-time transactional data from the inter-bank settlements system and CBN compliance data. In addition to more effective transaction monitoring, this new infrastructure, among other things, has the potential of making regulatory intervention more evidence-based.

7.3.2.4 Likelihood Assessment of ML Activity

Analytics tools can also be employed to assess the likelihood of ML activity in individual transactions. Coelho, De Simoni and Prenio\textsuperscript{91} list several examples of tools that have been developed by national authorities and their financial intelligence units. One example is Finland’s RAP’s tool that scores each suspicious activity report on the basis of different criteria such as the frequency involved parties have been reported, the existence of a criminal background or ongoing investigations.

7.3.3 Challenges

Coelho, De Simoni and Prenio\textsuperscript{92} note that new technologies give rise to several challenges. First, in light of the computational capacity required to treat large volumes of data can pose challenges in terms of computational capacity. Another challenge is the safeguarding of private and confidential data. A final challenge may be that machine learning-based tools become ineffective over time.

\textsuperscript{90} R2A (undated). Financial Authorities in the Era of Data Abundance: RegTech for Regulators and SupTech Solutions, white paper, pp. 36-37.


\textsuperscript{92} Ibid. p. 16.
7.4 Other Government-Driven Technological Solution

7.4.1 Digital Identification

Huw van Steenis, Chair of Sustainable Finance at UBS, recently argued\(^\text{93}\) that governments should champion digital forms of identification, following the example of India’s Aadhaar programme, which simplifies the process through which networks can know their customers. The FCA’s sandbox’s fifth cohort included several companies that looked at decentralised and federalised digital identity platforms machine learning identity verification.\(^\text{94}\) Such new identification mechanisms reduce the need for manual ID checks and help organisations avoid having to do duplicate checks.

7.4.2 Improved Information Sharing

Fighting financial crime networks requires cross-institutional and national collaboration and data sharing. There have been several initiatives working towards this end; an example is the FCA’s 2019 TechSprint\(^\text{95}\), which focused on how encryption techniques, so-called privacy enhancing technologies (PETs), can facilitate the sharing of information about ML and TF in compliance with data security laws.

Among the solutions participants presented where (1) federated learning technologies to share and identify financial crime typologies across multiple entities and (2) the use of PETs to pool data to allow for better identification of beneficial ownerships by eliminating discrepancies between public registers and firms’ own records.

---


7.5 International Technological Collaboration

Beyond the sandbox initiatives there have been broader attempts to enhance cross-border collaboration to fight financial crime. The most prominent example is the GFIN, a “network of 50 organisations committed to supporting financial innovation in the interests of consumers” that was formally launched in January 2019.96 In the FCA’s Megan Butler’s words, “it provides a forum for regulators and firms to collaborate on common challenges policy questions”.97

---

96 FCA (2019). Global Financial Innovation Network (GFIN)
8 Conclusion

ML and TF remain a serious challenge for governments on the African continent. Rapid technological change has in some instances accentuated the threats emanating from these categories of financial crime and financial authorities, just like elsewhere in the world, will have to invest considerable resources in AML/CTF measures. None of this has gone unnoticed in African countries and, to some extent, action has already been taken. However, measures remain incomplete and incoherent: there is a difference in employing new tool and turning it into an effective AML/CTF weapon. Among the most promising initiatives are probably, Nigeria’s Data Stack, which has created tremendous opportunities for a much more integrated, data-driven approach to fighting financial crime.
9 Bibliography


FATF (2013). *Prepaid Cards, Mobile Payments and Internet-Based Payment Services*, FATF (2013). Guidance for a Risk-Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services, June 2013, FATF/OECD.


Financial Intelligence Centre (undated). *Financial Intelligence Centre Guidance Note 4 on Suspicious Transaction Reporting*.


FCA (2019). Global Financial Innovation Network (GFIN)


Pedro de Morais, J. (2016), The fight against money laundering – an African perspective, opinion piece, 16/01/2016, Financial Times, webpage accessed on 02/12/2019: https://www.ft.com/content/c8184a87-0590-3aa9-b0af-2c6ba5f28c33


