JOURNAL OF ANTI-CORRUPTION LAW

2022 Volume 6 Number 1 Pages 127 - 152

GRAPPLING WITH THE SCOURGE OF MONEY LAUNDERING DURING THE COVID-19 PANDEMIC IN SOUTH AFRICA

Coleta Wesso* & Abraham Hamman**

ABSTRACT

The deadly COVID-19 pandemic has unfortunately presented new opportunities for perpetrators to exploit. As such, hefty amounts of economic crimes such as money laundering and money laundering threats were committed from the dawn of the COVID-19 pandemic, up to date of publication of this article. This criminal activity is highly likely to continue unless proficient solutions are efficiently activated and essentially carried out. This article sets out the ML and ML threat findings in South Africa as well as internationally during the pandemic, the South African anti-money laundering (AML) framework status quo, and what the way forward could be. The ultimate purpose of this article is to attempt to provide enlightenment on the topic and to offer thought and action provoking solutions on how similar future problems could be solved and addressed more effectively. It could also be a crucial contribution towards the government and society at large to be more prepared to not only grapple with, but also conquer the criminality of certain individuals.

1. INTRODUCTION

South Africa, often referred to as the Rainbow Nation, is granted miraculous landmarks, tourist attractions, lush vegetation, platinum metals, gold,[1] cultural diversity and beautiful citizens.[2] It is, however, incontestably and unfortunately so that with this said splendour,

* B.Com (Law), LLB, LLM (UWC), Attorney of the High Court of South Africa. Email: cjwprod@gmail.com. This article is based on Ms Wesso's LLM dissertation: Wesso C (2022) "An Analysis of the Challenges in Curbing and Combatting COVID-19 Related Money Laundering Threats and Vulnerabilities in South Africa".

** LLM, LLD (UWC), Associate Professor Department of Criminal Justice & Procedure Faculty of Law University of the Western Cape. Email: ajhamman@uwc.ac.za.

1 Let's Travel More (2 November 2018) "10 Things South Africa Is Famous For", available at https://lets-travel-more.com/10-things-south-africa-is-famous-for/ (visited 15 November 2021).

2 Morkel G (2 November 2021) "South Africa Has the Ninth Highest Number of 'Beautiful' People in the World – Study", available at https://www.news24.com/channel/the-juice/news/pageant/south-africa-has-the-ninth-highest-number-of-beautiful-people-in-the-world-study-20211102-2 (visited 15 November 2021).

detriment also resides. South African citizens and the rest of the world have endured numerous hardships during the COVID-19 pandemic.[3] The years 2019 to 2022, have, however, proven to be especially extraordinary in the history of humankind. The world is presently grappling with the deadly global COVID-19 pandemic. The disastrous effects that people had to cope with was exploited by criminals who saw a new avenue to commit crime. The emergency relief that was granted by various governments through legislation and various other means gave fraudsters, launderers, and corrupt government officials opportunities to pounce on this newfound source.

This discussion addresses the issue of how criminals really abused the opportunity and took the COVID-19 pandemic situation provided to them to commit crime. The specific focus is on how South Africa and the rest of the world was unable to escape the atrocious grip of Money Laundering (ML). ML works hand in hand with other crimes, known as predicate offences. ML converts the illegal proceeds into legitimate proceeds, and in doing so, conceals the predicate transaction.[4] Predicate offences are thus always to be kept in mind when alluding to ML and its threats.[5]

ML is the unlawful method of converting 'dirty' proceeds, produced from predicate offences, into 'clean' proceeds that can seemingly be used at liberty in legitimate business operations without being hidden from any regulatory authorities.[6] ML is shockingly prevalent throughout the world. It is a process that has overwhelmingly distressed society for ages. The ML crimes committed during the COVID-19 pandemic are an example of how criminals took advantage of a vulnerable situation. This article could be an important contribution in that should similar future pandemics or disasters occur, the South African government will be more prepared to deal with the criminality of certain individuals. It furthermore essentially is an attempt to offer some solutions on how similar future issues could be solved and addressed more effectively in the country. The money laundering trends in South Africa are referred to in detail. The flagship findings and guidelines of the FATF in relation to the COVID-19 pandemic will also be discussed. The next section will closely examine the ML and ML threats in South Africa during the COVID-19 pandemic.

3 Some hardships may be the same or similar, and some may be completely different.

4 Goredema C (2004) "Money Laundering in Southern Africa Incidence, Magnitude and Prospects for its Control" at 1.

5 Although many other predicate crimes, such as corruption, fraud and theft were committed during the pandemic, the focus of this article is on the money laundering and money laundering threats prevalent during the COVID-109 pandemic.

6 CFI (2021) "Money Laundering", available at https://corporatefinanceinstitute.com/resources/knowledge/finance/money-laundering/ (visited 14 June 2022).

2. COVID-19 MONEY LAUNDERING TRENDS AND THREATS IN SOUTH AFRICA

The COVID-19 pandemic has resulted in a lengthy and peculiar journey for most of the financial crime compliance industry in South Africa. It is a journey distinguished, not only by confusion and commotion, but also adaptation and innovation. Fraudsters and money launderers have speedily adjusted to the COVID-19 pandemic reality. The Zondo Judicial Commission of Inquiry into State Capture (the Zondo Commission) dealt with shockingly extensive fraud which took place throughout the tenure of former president of South Africa, Jacob Zuma.[7] Apart from what is being revealed at the Zondo Commission, the fact that the COVID-19 pandemic never stopped the treacherous ways of criminals in South Africa, is distressing.

During 2020 the South African government banned tobacco sales. This caused an immense influx of illegal cigarettes into the market. Criminal syndicates generated enormous amounts of proceeds. Former SA Revenue Services (SARS) executive Johann van Loggerenberg states that the South African Government had inserted over R2 billion into the illegitimate economy during that lockdown period.[8] This involved cash that was unrecorded, unaccounted for and never to be recovered. This is an illustration of the huge amount of cash that needed to be laundered in order to be reintegrated into the economy. Loggerenberg further stated: "Crooks have made over R 2 billion within two months. Lord alone knows what they will do with it in future."[9]

To make matters worse, the very entity that obligates itself to the establishment of a safe and protected environment for all people in South Africa[10] is unfortunately tainted with fraud and corruption. It was discovered that, in the space of only six months in 2020, irregular PPE procurements to the amount of R1.6 billion took place in connection with the South African Police Services (SAPS).[11] The obstinate high-level fraud and corruption at the SAPS truly

7 Imray G (15 March 2021) "Hope that South Africa's COVID-19 Corruption Inspires Action" *AP News*, available at https://apnews.com/article/government-contracts-cape-town-coronavirus-pandemic-africa-south-africa-c59e9fa1906b5622d38947e327fb6b6d (visited 16 June 2022).

8 Haffajee F (12 June 2020) "Dlamini Zuma Turns Cigarettes into Illicit Drugs as the Underground Economy Takes Over" *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2020-06-12-dlamini-zuma-turns-cigarettes-into-illicit-drugs-as-the-underground-economy-takes-over/ (visited 16 June 2022).

9 Haffajee (12 June 2020).

10 South African Police Service (2021) "About Us", available at https://www.saps.gov.za/about/about.php (visited 16 June 2022).

11 Thamm M (30 May 2021) "SAPS blew R1.6bn in irregular PPE expenditure from March to August 2020, confidential internal audit uncovers" *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-05-30-saps-blew-r1-6bn-in-irregular-ppe-expenditure-from-march-to-august-2020-confidential-internal-audit-uncovers/ (visited 16 June 2022).

deprives South Africans of the right to safety.[12] It also plunders the reputation of SAPS practitioners who are virtuous and duty driven employees.

With the nature of the COVID-19 pandemic increasing the usage of the internet, there has been a massive surge in digital financial crime. An example of the detriment caused by this is the fact that in 2020, more than R500 million was lost in debit card scams in South Africa. This comes as a result of the 2020 crime statistics released by the SA Banking Risk Information (Sabric) on 29 September 2021.[13] It was reported that in comparison to 2019, digital crime occurrences increased by 33 per cent in 2020. Debit card fraud took place via various approaches. These include the usage of false applications amounting to R4.8 million; account takeovers totalling R1.6 million; lost or stolen debit cards adding up to R193 million; a 'card not present'[14] method to the amount of R278 million; non-receipt of issued debit cards to the value of R484 983; and counterfeit debit cards worth R39.5 million.[15] It is moreover indicated that the main technique used by criminals when targeting victims is social engineering which encompasses deception in order to manipulate an individual to avail confidential or personal information. Examples of this is phishing whereby a fake email, which seems authentic, is utilised in an attempt to acquire personal information including card numbers and passwords. Vishing, which is the use of fake SMSs or phone calls, is used for the same aforementioned purpose but includes the attempt to attain one-time passwords.[16] It was found that criminals instigated spoof emails offering PPE like sanitizers, vaccines or masks. People were led to phishing websites through clicking on links to these emails. They were then provoked to provide banking details, which, in turn, resulted in criminals transacting with that information without permission.[17]

South African life insurance companies also discovered that there has been an increase in insurance fraud cases as a result of the COVID-19 pandemic. According to the Association for Savings and Investment South Africa (Asisa), 3 186 claims, totalling R587.3 million were recorded in comparison to the 2 837 claims amounting to R537.1 million in 2019.[18] The

12 Thamm (30 May 2021).

13 Smith C (29 September 2021) "Over Half a Billion Rand Lost in Debit Card Scams in SA Last Year", available at https://www.news24.com/fin24/companies/financial-services/over-half-a-billion-rand-lost-in-debit-card-scams-in-sa-last-year-20210929 (visited 16 June 2022).

14 A card not present transaction (CNP) takes place when the credit card or cardholder is not physically present at the time of the transaction. An example of this includes orders that occur remotely via the internet. See Galante M (26 December 2017) "What Is a Card-Not-Present (CNP) Transaction and Why It Costs More", available at https://squareup.com/us/en/townsquare/what-is-a-card-not-present-transaction (visited 16 June 2022).

15 Smith (29 August 2021).

16 Ibid.

17 Ibid.

18 Hesse M (31 August 2021) "A Surge In Insurance Fraud Cases as SA Struggles During the Pandemic", available at https://www.iol.co.za/personal-finance/insurance/a-surge-in-insurance-fraud-cases-as-sa-struggles-during-the-pandemic-52b1ccd5-e44e-4128-a2b3-bb1697a6a6e8 (visited 16 June 2022).

convenor of the Asisa Forensics Standing Committee, Megan Govender, stated that the surge is not startling because the hard-hitting economic circumstances have caused temptation for deceitful syndicates and policyholders to attempt obtaining insurance pay-outs. It was found that the chief prevalence of fraud in 2020, concerning 2 282 claims, was related to funeral policies.[19]

Furthermore, between June and August 2020, the Gauteng Department of Education was entwined with suspicious dealings involving the spend of over R431 million on the sanitising of schools. These proceeds were paid to hundreds of companies in sundry payments.[20] Sundry income is produced from sources other than a company's usual business operation**.** It is also referred to as other operating income or miscellaneous income. Sundry income is frequently seen as irregular. Over the long term, it is also not a guaranteed source of company income.[21] Many of the aforesaid companies involved with the Gauteng Department of Education debacle give the impression that they have no proficiency or erstwhile immersion in the cleaning industry. Aggravating the circumstances, was the fact that these transactions were for a type of 'decontamination' and 'deep cleaning' that was not recommended nor necessitated by either the Department of Basic Education (DoBE) or the Department of Health (DoH).[22]

Moreover, in order to speed up investigations into duplicitous claims at the Unemployment Insurance Fund (UIF), the portfolio committee on employment and labour called upon law enforcement agencies. Suspect claims totalling 75 were investigated, one of which related to the theft of R5.7 million from the COVID-19 relief fund initially intended for 1 400 employees to receive.[23] Specifically, a bookkeeper of 39 years of age was also arrested in connection with defrauding the UIF COVID-19 relief scheme namely the COVID-19 Temporary Employer-Employee Relief Scheme (TERS). This bookkeeper allegedly swindled R11.1 million out of the COVID-19 TERS.[24] Furthermore, Democratic Alliance (DA) councillor, Nora Grose, and Atlantis

19 Hesse (31 August 2021).

20 Heywood M (26 January 2021) "Gauteng Department of Education spent R431-million in three months on unnecessary 'deep cleaning' and 'decontamination' of schools'" *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-01-26-gauteng-department-of-education-spent-r431-million-in-three-months-on-unnecessary-deep-cleaning-and-decontamination-of-schools/ (visited 16 June 2022).

21 Kenton W (6 September 2019) 'Sundry Income', available at https://www.investopedia.com/terms/s/sundryincome.asp#:~:text=Key%20Takeaways,income%20over%20the%20long%20term (visited 16 June 2022).

22 Heywood (26 January 2021).

23 Mabuza E (8 July 2020) "75 UIF Fraud Cases Under Investigation, MPs Call for Speedy Results" *Times Live*, available at https://www.timeslive.co.za/news/south-africa/2020-07-08-75-uif-fraud-cases-under-investigation-mps-call-for-speedy-results/ (visited 16 June 2022).

24 Buthelezi L (27 August 2021) "Bookkeeper Who Allegedly Scammed UIF out of R11.1m in Covid-19 Grants Due in Court on Tuesday", available at https://www.news24.com/fin24/economy/bookkeeper-who-allegedly-scammed-uif-out-of-r111m-in-covid-19-grants-due-in-court-on-tuesday-20210827 (visited 16 June 2022).

pastor, Reuben Swartz, have been charged with fraud and ML in connection with the TERS as well as money that was meant for food parcels, being channelled to the Life Changers Church in Table View, Western Cape.[25]

Yet another example of possible fraud in South Africa during COVID-19 was when PPE was astoundingly found dumped in a river that passes through Irene, Centurion, Johannesburg. This PPE was intended to protect health workers and restrain the spread of COVID-19. Nehawu spokesperson Khaya Xaba stated that they believe this formed part of the tenders that were issued illegally and PPE's that were produced mediocrely. The matter was directed to the applicable institutions for investigation purposes following reports of enormous tender indiscretions and looting.[26]

Additionally, Dr Zweli Mkhize, former South African Minister of Health, his close associates, Tahera Mather and Naadhira Mitha,[27] as well as his family members were said to also have pocketed COVID-19 proceeds in connection with a fraudulent contractor selected by the DoH.[28] The company, Digital Vibes, secured contracts worth over R150 million for work in connection with the COVID-19 pandemic.[29] The firm obtained the orders from the DoH for the COVID-19 projects in just nine months.[30] Apparently and quite interestingly, Digital Vibes had no website. According to company records, its business address is recorded as a residential property in KwaDukuza, previously Stanger, on the Northern Coast of KwaZulu-Natal.[31] Radha Hariram, the company's principal director, did not seem to have any observable track record in the communications sector.[32] Following this, Mkhize resigned from his position as South African Minister of Health.[33] On 29 September 2021, the SIU's report

25 Charles M (30 August 2021) 'DA Ward Councillor Charged with TERS Fraud, Money Laundering Back in Court' *News24*, available at https://www.news24.com/news24/southafrica/news/da-ward-councillor-charged-with-ters-fraud-money-laundering-back-in-court-20210830 (visited 16 June 2022).

26 Ntshidi E (2 August 2020) "Nehawu: 'Tenderpreneurs' Likely Behind Dumped PPEs Found in Centurion" *EWN*, available at https://ewn.co.za/2020/08/03/nehawu-tenderpreneurs-likely-behind-dumped-ppes-found-in-centurion (visited 16 June 2022).

27 Bhengu C (29 September 2021) "Five shocking revelations from the SIU report on Digital Vibes" *Times Live*, available at https://www.timeslive.co.za/news/south-africa/2021-09-29-five-shocking-revelations-from-the-siu-report-on-digital-vibes/ (visited 16 June 2022).

28 Myburgh PL (23 February 2021) "Zweli Mkhize's 'Family Friend' and Ex-Private Secretary Pocket Covid-19 Cash Via R82m Department of Health Contracts" *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-02-23-zweli-mkhizes-family-friend-and-ex-private-secretary-pocket-covid-19-cash-via-r82m-department-of-health-contracts/ (visited 16 June 2022).

29 Naidoo J (29 September 2021) "WATCH: Digital Vibes's non-existent office tip of the iceberg" *IOL*, available at https://www.iol.co.za/news/politics/watch-digital-vibess-non-existent-office-tip-of-the-iceberg-6c5fa0f0-31c8-459d-a6ad-c8b3e84dfd37 (visited 16 June 2022).

30 Myburgh (23 February 2021).

31 Ibid.

32 Ibid.

33 Pillay K (5 August 2021) 'Zweli Mkhize resigns over Digital Vibes scandal' *IOL*, available at https://www.iol.co.za/news/politics/zweli-mkhize-resigns-over-digital-vibes-scandal-8643a0df-74f1-4696-856d-408ea37610d2 (visited 16 June 2022).

on Digital Vibes was finally released which directly implicated the former health minister and his family, as well as Mather and Mitha.[34] To have the SIU findings set aside, Mkhize has since launched a court bid on the grounds of the SIU's investigation amounting to a "witch-hunt".[35]

Via entities directly and indirectly linked to him, businessman, Hamilton Ndlovu, also illegitimately won approximately R172 million in PPE contracts from the National Health Laboratory Service (NHLS). The SIU stated that the issue was raised with them in August 2020 subsequent to a R72 million tender involving the provision of PPE which was awarded to entities owned by Ndlovu and Feliham, a company belonging to the fiancé of Ndlovu. Feliham was restricted via the Central Supplier Database (CSD) from engaging in business with the state. The SIU's probe revealed, however, that officials at the NHLS "circumvented this restriction and awarded a contract to Feliham worth R14 475 500 for 2 500 000 surgical shoe covers". The SIU furthermore found inter alia that Ndlovu was indirectly connected to several other entities and that, by way of irregular procurement procedures, the entities were all given contracts by the NHLS. Ndlovu bought five luxury cars in one day and, in 2020, after posting a video of his luxurious vehicles including a Lamborghini Urus, a Jeep Grand Cherokee and three Porsches, Ndlovu made headlines.[36]

Moreover, in January 2021 it was stated that 57 contracts for the procurement of PPE by the KZN Department of Education (DoE) worth R492.6 million was originally investigated by the Special Investigating Unit (SIU) in South Africa. This included 18 contracts for the procurement of PPE by the Department of Social Development (DSD) to the value of R21.2 million and four contracts for the procurement of blankets by the DSD to the value of R 22.4 million.[37] Swelling the sum of contracts under investigation to 226 totalling R606 435 294 in value, the SIU had further added the contracts of numerous KwaZulu-Natal municipalities and the Office of the Premier to its COVID-19 investigations in the province.[38] In addition to this, Kaizer Kganyago, the SIU's head of stakeholder relations and communications, had indicated that many further

34 Myburgh PL (29 September 2021) 'Released: Damning SIU Report Finds at Least R72m Fruitless and Wasted, Implicates Mkhize, DoH Officials in Digital Vibes Contract' *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-09-29-released-damning-siu-report-finds-at-least-r72m-fruitless-and-wasted-implicates-mkhize-doh-officials-in-digital-vibes-contract/ (visited 16 April 2022).

35 Davis R (19 October 2021) 'Digital Vibes Scandal: The Story Behind the Story', available at https://www.dailymaverick.co.za/article/2021-10-19-digital-vibes-scandal-the-story-behind-the-story/ (visited 16 April 2022).

36 Pijoos D (27 January 2022) 'How Flashy Businessman Hamilton Ndlovu Scored Close to R172 Million in Irregular PPE Tenders' *News24*, available at https://www.news24.com/news24/southafrica/news/how-flashy-businessman-hamilton-ndlovu-scored-close-to-r172-million-in-irregular-ppe-tenders-20220127 (visited 7 June 2022). See also *Special Investigating Unit and Another v Ndlovu and Others* (GP 19 of 2021) [2022] ZAST 6 (7 June 2022).

37 Erasmus D (15 January 2021) 'KZN probe expanded: Covid-19 contracts worth over R600m now also being investigated' *Daily Maverick*, available at https://www.dailymaverick.co.za/article/2021-01-15-kzn-probe-expanded-contracts-worth-r600m-now-also-being-investigated/ (visited 19 June 2022).

38 Ibid.

contracts were also being investigated including nine contracts involving the Office of the Premier to the value of R1 122 550; 13 contracts relating to the uMngeni Municipality valued at R7 805 588; 59 contracts concerning the KwaDukuza Municipality totalling R4 190 501; 64 contracts linked to the eThekwini Municipality to the value of R53 214 200; and two contracts in connection with the Office of the Premier (Department of Transport (DoT)) totalling R3 902 455 in value.[39]

On 25 January 2022, a new report published by the SIU presented that a large number, in fact more than half of COVID-19 procurement contracts entered into by the government, were untoward. The report places concentration upon procurement by all spheres of the government regarding services, works and goods linked to the COVID-19 pandemic. As part of its task, the SIU probed 5 467 contracts awarded to 3 066 service providers totalling an amount of R14.3 billion. Investigations have been concluded concerning 4 549 contracts. The SIU found 2 803 of these contracts to be improper. Of the finalised investigations, this totals 62 per cent.[40]

It is evident that the COVID-19 pandemic has created a fertile environment not only for mental and physical impairment and fatality, but also in fact for the facilitation of ML. The aforementioned practical examples sorely illustrate the low levels to which criminals will stoop in order to carry out ML and ML threats. It also signifies the massive amounts of money involved in both the fraudulent activity as well as the investigation thereof. Criminals in order to use the money without impunity must deposit the money into the legitimate economy, without the scent of illegality. They then need to come up with ways to launder the money to receive the benefit without any chance of arrest and prosecution.

2.1 Findings by Corruption Watch (CW)

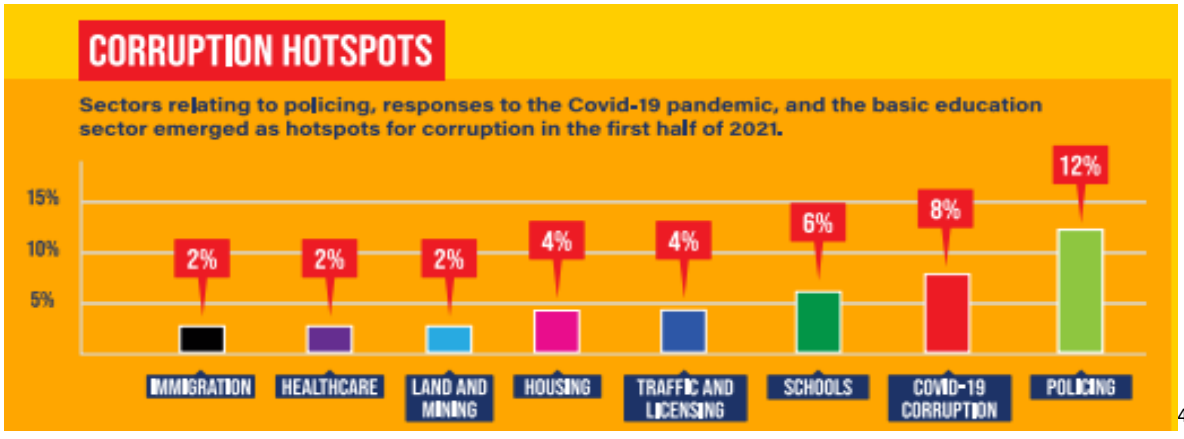
Corruption Watch provided a streamlined overview of the most common types of corruption during the COVID-19 pandemic and made specific statistical conclusions. These findings highlight the most pertinent problems that South Africa is currently facing regarding corruption which is in most instances a predicate crime for money laundering. On 21 September 2021, CW released its 2021 Analysis of Corruption Trends (ACT) report and podcast (the 2021 ACT), revealing the relentless magnitude of continued corruption during the first half of 2021. The 2021 ACT indicates that, in both the private and public sectors, 1 964 whistleblowers reported corruption. These actions of bravery often led to life threatening consequences. The 2021 ACT further states that the organisation received various reports including inter alia COVID-19 associated irregularities, school principals forcing sexual favours

39 Ibid.

40 Staff Writer (25 January 2022) 'More than Half of Government's Covid Contracts Under Investigation were Irregular: SIU' *Business Tech*, available at https://businesstech.co.za/news/government/552980/more-than-half-of-governments-covid-contracts-under-investigation-were-irregular-siu/ (visited 16 April 2022).

from temporary teachers to safeguard their jobs, and abuse of authority by the police. These reports emphasise the complicity between the private and public sectors.[41]

In terms of corruption levels per sector, most reports, amounting to 12 per cent of all reports, are linked to police corruption. This underlines the unceasing corruption dilemma in the policing sector which is further worsened by the powers endowed to the police whilst lockdown regulations were in effect. This is followed by eight per cent of reports which allude to corruption regarding procurement and maladministration associated with the COVID-19 pandemic, such as maladministration with TERS funding. Moreover, six per cent of reports are in connection with corruption in schools. Numerous whistleblowers in Gauteng, Limpopo and the Eastern Cape reported abuse of authority, normally by principals and the chairpersons of school governing bodies.[42] Also reported in this regard were irregularities in employment procedures and the theft or embezzlement of school funds. Additionally, four per cent of reports refer to corruption in public housing. Gauteng and the Western Cape emerged as hotspots of public housing corruption, where most whistleblowers exposed irregularities in the allocation of RDP houses, fraud in relation to the housing waiting lists, and abuse of authority. Alarmingly, it was also reported that corruption still occurs in regard to food parcels.[43] The bar graph below details the percentages of the corruption sector hotspots as mentioned above.



[44]

Source: Corruption Watch, 2021

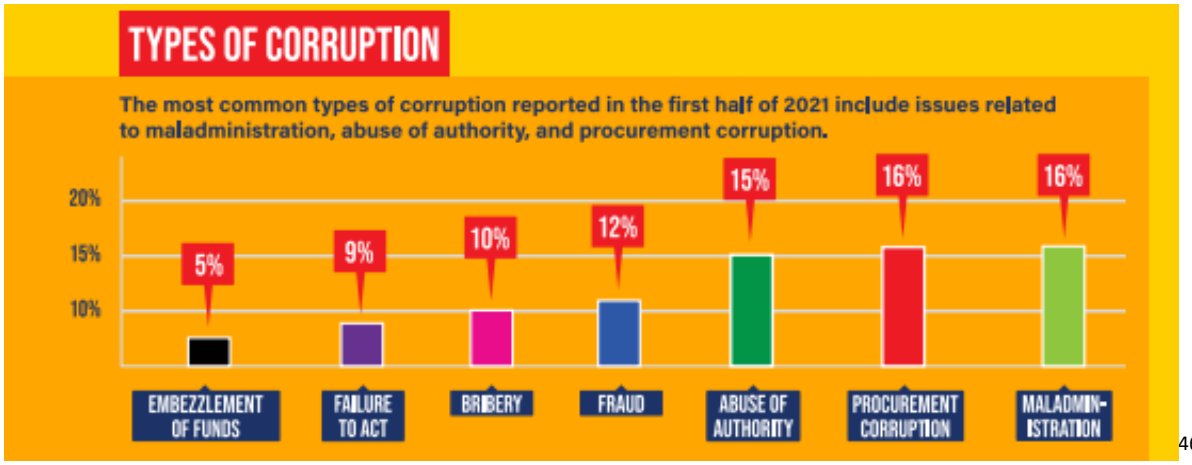
41 Corruption Watch (21 September 2021) 'New Corruption Report Exposes Continued Rot In Public And Private Sectors', available at https://www.corruptionwatch.org.za/new-corruption-report-exposes-continued-rot-in-public-and-private-sectors/ (visited 18 April 2022).

42 Ibid.

43 Ibid.

44 Ibid.

Turning to the most common types of corruption experienced, the 2021 ACT specifies that these include maladministration at 16 per cent, procurement corruption at 16 per cent, and the abuse of authority at 15 per cent. According to the organisation, these statistics indicate that attempts by the private and public sectors to deal with the corruption problem in South Africa are extremely insufficient.[45] The bar graph below illustrates the abovementioned most frequently occurring types of corruption.

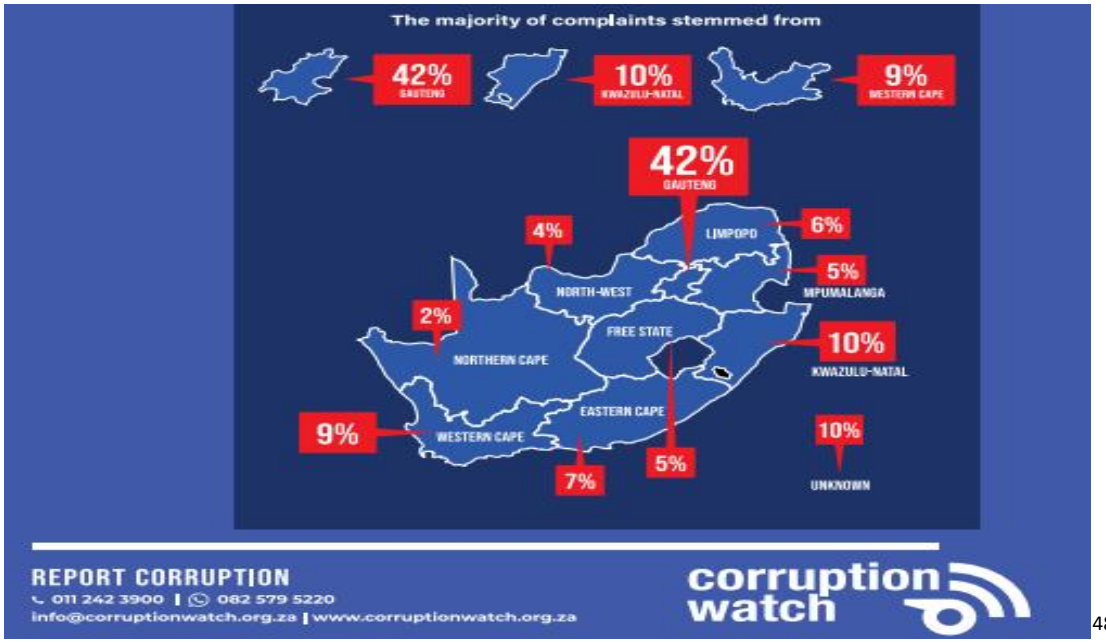


[46]

Source: Corruption Watch, 2021

On further analysis, the 2021 ACT reveals that most complaints, amounting to 42 per cent of the total reports, came from Gauteng. This was followed by KwaZulu-Natal at ten per cent, the Western Cape at nine per cent and the Eastern Cape totalling seven per cent. [47] The illustration below presents where the majority of complaints stemmed from.

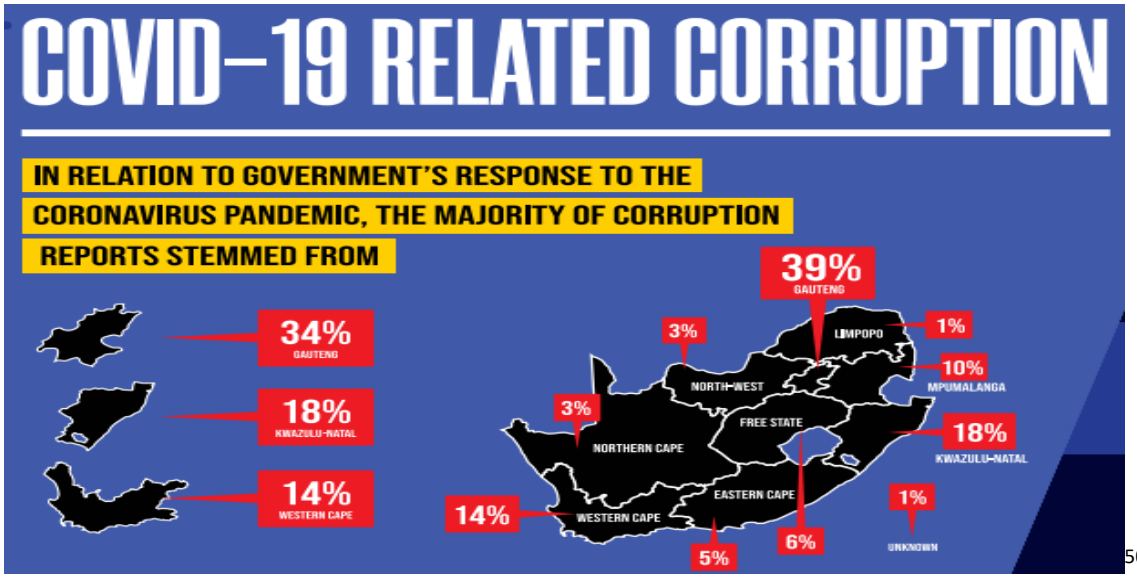
45 Ibid.
46 Ibid.
47 Ibid.



[48]

Source: Corruption Watch, 2021

Interestingly, corruption reports detailing government's retort to the COVID-19 pandemic transpired in Gauteng at 34 per cent, KwaZulu-Natal at 18 per cent, the Western Cape at 14 per cent, and Mpumalanga at ten per cent.[49] The illustration below displays this COVID-19 related corruption.



[50]

Source: Corruption Watch, 2021

48 Ibid.
49 Ibid.
50 Ibid.

The link between the COVID-19 pandemic and a surge in ML and ML threats is indeed clear from what has been highlighted in the 2021 ACT. Considering all the findings, Melusi Ncala, researcher at CW and author of the 2021 ACT stated: "This continues to be the story of corruption in South Africa according to almost 2 000 brave whistleblowers." He then asks: "So when will the tide turn?"[51] This is indeed a relevant question that truly reflects what many South Africans currently struggle with and desperately seek answers and guidance to. The FATF provides guidance in regard to ML and ML threats during the COVID-19 pandemic. It elaborates upon global ML risks, practical examples, and proposed actions during the COVID-19 pandemic. This is valuable information for South Africa, being a member of the FATF, to be cognisant of. The next section will thus focus on the FATF's response.

3. COVID-19 money laundering and money laundering threats identified by the FATF

Being the international standard setter for contesting ML, TF, and the proliferation thereof,[52] the FATF, in collaboration with its observers and members, have acted rapidly amid the COVID-19 pandemic. They have done so with the purpose of addressing the susceptibilities incipient from the global catastrophe in relation to ML.[53] Though not discussed in any detail this article, it is important to highlight the fact that the FATF took initiative by releasing various COVID-19 statements[54] and furthermore arranging a series of webinars, involving participants from both the private and public sectors, to raise awareness and discuss emerging risks.[55] However, attention in this section will be drawn to the FATF's paper issued in May 2020 addressed together with the paper update issued by the FATF in December 2020, as well as the FATF's 18 January 2021 Statement. The papers and statement present a collective global response to ML and TF associated with the COVID-19 pandemic.[56] Due to the length of the papers and statement, reference will be made to the sections which are possibly the most applicable to the findings relating to South Africa. Although not specifically mentioned in the FATFs responses, possible links between what occurred in South Africa and what the FATF mentions, will be made.

51 Ibid.

52 FATF (1 April 2021) 'Statement by the FATF President: COVID-19 and measures to combat illicit financing', available at https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html (visited 16 June 2022). See also FATF (2020) "Annual Report 2020-2021" at 5.

53 FATF (2021) 'FATF focus on COVID-19', available at https://www.fatf-gafi.org/publications/covid-19/covid-19.html?hf=10&b=0&s=desc(fatf_releasedate) (visited 16 June 2022).

54 FATF (1 April 2020). FATF (23 October 2020) 'The Importance of Allocating Sufficient Resources to AML/CFT Regimes During the COVID-19 Pandemic', available at https://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-impact-oct-2020.html (accessed on 16 June 2022).

55 FATF (2021).

56 Ibid.

As previously mentioned, the unparalleled and hastily developing COVID-19 pandemic has impelled the creation of the May 2020 COVID-19 related Money Laundering and Terrorist Financing Risks and Policy Responses Paper (FATF May 2020 Paper).[57] It is an integral fragment of a timely and synchronised retort to the effects of the COVID-19 health crisis on global AML / Combatting the Financing of Terrorism (CFT) efforts and the application of the FATF Standards especially amid the current global catastrophe.[58] This paper is informed by information accumulated from open-source research and FATF observer organisations such as the International Monetary Fund (IMF), the United Nations and the World Bank as well as member countries of the FATF and FATF-Style Regional Bodies (FSRB)s.[59] There are three wide-ranging themes that this paper focuses upon which includes the evolving ML / FT risks, current COVID-19 impacts on AML / CFT regimes, and possible AML / CFT responses for deliberation.[60] The FATF has, since May 2020, perpetuated the collection and assessment of pertinent information on the ramifications of the COVID-19 pandemic.[61] The assessments seen in the December 2020 Paper Update regarding COVID-19-related Money Laundering and Terrorist Financing (FATF December 2020 Paper Update) reaffirms the continued relevance of the risks and policy feedback.[62] The objective of the FATF December 2020 Paper Update is to provide supplementary information on COVID-19 associated ML and TF hazards to reporting entities, other private sector entities, as well as further stakeholders.[63]

Turning to the findings, it is stated that the COVID-19 pandemic has explicably engendered several government responses. Though the exact circumstances and public health responses in every respective country contrast in accordance with the impact of the COVID-19 pandemic, the embryonic risk depiction detailed in these papers is based on the following general assumptions.[64] Individuals, businesses and governments are progressively turning to online technology in order to socially interact and work remotely; industries that are declared non-essential have physically closed; and both non-essential and essential industries have had larger online sales.[65] Furthermore, there is a massive need for medical supplies amid a global shortage due to extreme demand; financial institutions including banks are limiting in-person banking; and lockdown and other measures have caused the laying off of workers or mass unemployment, harm to government revenue and an over-all economic recession. This influences the social and financial conduct of businesses and individuals.[66] Moreover,

57 FATF (May 2020) at 5.
58 Ibid.
59 Ibid.
60 Ibid.
61 FATF (December 2020) at 5.
62 Ibid.
63 Ibid.
64 Ibid.
65 Ibid.
66 Ibid.

resources are removed from other areas of work due to governments having to reprioritise resources in response to the COVID-19 pandemic. In addition, since individual travel and international trade volumes are limited, conventional multinational organised crime structures exploit the traditional illegitimate revenue schemes of organised crime groups and global supply chains, which are affected by the COVID-19 pandemic. While inadvertent, these measures create new prospects for criminals and terrorists to generate and then launder unlawful profits.[67]

These general assumptions and aspects are also reflected in South Africa. It is understood that the ML and ML threats that South Africa is grappling with during the COVID-19 pandemic include, but are not limited to, maladministration, procurement corruption, fraud, abuse of power, bribery, employment corruption, dereliction of duty, embezzlement of funds, lockdown fraud, insurance fraud, digital fraud and fraud and ML involving places of worship. This then also comprises aspects such as procurement irregularities, compliance issues and fraudulent activities in various businesses, agencies, state institutions and departments. These forms of ML and ML threats have occurred mostly in the SAPS, government response to the COVID-19 pandemic, school, and housing sectors. Following the assumptions, the next section of this article will highlight the evolving ML risks identified by the FATF. It will do so by probing into the FATF May 2020 Paper and will simultaneously intertwine findings of the FATF December 2020 Paper Update whilst concurrently linking possible indications in relation to the South African ML and ML threat findings during the COVID-19 pandemic.

3.1 Amplified fraud

The aspects reported by the FATF open sources, observers, and members, point to criminals attempting to profit from the COVID-19 pandemic through increased fraudulent activities.[68] An increase in fraudulent activity is similarly identified in South Africa. The activities uncovered by the FATF include an increase in fundraising for fake charities whereby emails, distributed by criminals pretending to be international charities or organisations, request donations for victim, product and / or research based fundraising campaigns linked to COVID-19. Through the suspect's secure digital wallet, credit card details or payments are requested to be given or made by the recipients of these emails.[69] In South Africa it was also noted that fraudulent activities and ML took place in connection with the Life Changers Church in Table View, Western Cape.

67 FATF (May 2020) at 6.
68 FATF (May2020) at 6 and 7.
69 Ibid.

Another activity is the impersonation of officials. With the purpose of acquiring physical cash or personal banking details, criminals contact individuals via email, telephonically or in person and mimic officials. Impersonation may occur in the form of criminals acting as government officials and intreating personal banking details for the purpose of tax relief,[70] or they act as hospital officials who claim that a family member is ill and they are in need of a payment for treatment.[71] These impersonations are said to increase because criminals endeavour to benefit from the profits of grant and tax relief payments by governments around the globe to their citizens.[72] It is likely that these occurrences could be found in the SAPS fraudulent activity in South Africa where statistics have shown that there indeed was dereliction of duty, abuse of power and bribery.

Known as further fraud increasing activity is the counterfeiting of, amongst others, essential goods including medicines, medical supplies, pharmaceutical products and personal protective equipment.[73] Offering testing kits, masks and other products, criminals that maintain that they are employees of charities, international organisations or businesses request credit card details for a shipping fee or a payment but then fail to distribute the goods.[74] Victims are in some instances requested to, via bank transfers, provide payments in advance. They would then be directed to collect the goods from various places only to be informed on arrival that there was actually no such arrangement made.[75] Similarly, in some instances the goods are distributed to the consumer, however, they are ineffective or forged. There is also an increase in deceptive COVID-19 treatment claims and sales in illegal products advertised as miracle cures.[76] South Africa can certainly relate here as there were findings of massive PPE fraud and even instances where massive amounts of seemingly counterfeit PPE were dumped in a river located in Johannesburg.

---

70 FATF (May 2020) at 6. See also US Treasury (2020) 'COVID-19 Scams', available at https://home.treasury.gov/services/report-fraud-waste-and-abuse/covid-19-scams (visited 16 June 2022).

71 FATF (May 2020) at 6. Interpol (13 March 2020) 'Criminals Taking Advantage of Coronavirus Anxiety to Defraud Victims Online', available at https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraud-linked-to-COVID-19 (visited 16 June 2022). See also Interpol (14 April 2020) 'Unmasked: International COVID-19 Fraud Exposed', available at https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed (visited 16 June 2022).

72 FATF (May 2020) at 6.

73 Ibid.

74 Ibid.

75 FATF (May 2020) at 6. See also Singapore Police Force (2020) 'Singapore Police Force Police Advisory – New Type of E-Commerce Scams Involving The Sale Of Face Masks', available at https://www.police.gov.sg/Media-Room/News/20200222_OTHERS_New_Type_Of_ECommerce_Scams_Involving_The_Sale_Of_Face_Masks (visited 16 June 2022).

76 FATF (May 2020) at 6.

Amidst the COVID-19 pandemic, scams, through fundraising for false charities, have continued according to the FATF December 2020 Paper Update. Criminals fool victims by using social media podia to request funds or they contact individuals, misrepresent themselves and demand money for fake or imaginary charities.[77] These impostors sometimes betray victims by creating false charities or by deceptively claiming that they were representatives of renowned international charities.[78] South Africans are found to be victims of digital fraud and are thus also prone to the social media dangers as discussed in the next section.

3.2 Cyber-crime attacks

Another augmented ML threat identified in this paper is Cyber Crime. This is an aspect that South Africa has also grappled with in relation to digital fraud during the COVID-19 pandemic, as mentioned previously. The FATF indicates that there has been a strident upsurge in social engineering attacks largely due to the remote working element. These attacks include phishing via email and mobile messages. To insert malicious software,[79] otherwise known as malware, on mobile devices or personal computers, impostors are taking advantage of COVID-19 concerns. An example of this is where criminals impersonate government through SMSing to entice individuals to duplicitous government websites with the purpose of gaining usernames, passwords and / or other personal account details.[80] A further example is where cyber fraudsters, by impersonating the WHO and distributing mobile messages and emails, lead victims to open attachments or click on malevolent links which would, in turn, divulge the person's password and username.[81]

Cyber-attacks also include business email compromise scams whereby cyber criminals exploit the vulnerabilities in the network security of businesses to achieve entry into customer transaction and contact details. Once the information is obtained, it is then utilised via phishing emails for criminals to act as the business and demand payment for the valid services and / or goods. The payment is transferred into the illegal accounts of these criminals.[82] In a

77 FATF (December 2020) at 13.

78 Ibid.

79 FATF (May 2020) at 7. See also Fruhlinger J (17 May 2019) 'Malware Explained: How to Prevent, Detect and Recover from It', available at https://www.csoonline.com/article/3295877/what-is-malware-viruses-worms-trojans-and-beyond.html#:~:text=Malware%2C%20short%20for%20malicious%20software,gain%20access%20to%20sensitive%20information (visited 16 June 2022).

80 FATF (May 2020) at 7. See also CISA (8 April 2020) 'COVID-19 Exploited by Malicious Cyber Actors', available at https://us-cert.cisa.gov/ncas/alerts/aa20-099a (visited 16 June 2022).

81 FATF (May2020) at 7. See also WHO (2020) 'Beware of Criminals Pretending to be WHO', available at http://www.who.int/about/communications/cyber-security (visited 16 June 2022).

82 FATF (May 2020) at 7. See also FBI (6 April 2020) 'FBI Anticipates Rise in Business Email Compromise

further instance, under the ploy of paying for bulk supplies of hand sanitiser and surgical masks, a company received hoaxed emails akin to those distributed by their business partner (company and partner details omitted by the FATF). The intention of this is to transmit payment transfers to the controlled bank accounts of fraudsters.[83]

Additional cyber-attacks identified are ransomware attacks. Ransomware is software that is able to demand a ransom for a computer's release after locking it.[84] Various methods of inserting ransomware into mobile devices or personal computers are reportedly what criminals are now also involved in. By means of fraudulent mobile applications and websites that seem to share COVID-19 related information, cybercriminals obtain and lock admission to victims' devices until payment is acquired. Organisations leading the COVID-19 response, particularly hospitals and other medical institutions have progressively become targets of cybercriminals for attacks relating to ransomware.[85]

It was confirmed in the FATF December 2020 Paper Update that a large number of global reports indicate a continuous rise in cyber-related fraud. There are concerns predominantly regarding ransomware attacks, business email compromise schemes, and email and SMS phishing scams.[86] It is important to also note that the COVID-19 associated email and SMS phishing schemes have shifted according to individuals' interests and governments' actions and adaptations over time. Emails with false links now tend to refer to bank distributing aids, government stimulus packages, websites selling masks, and infection rate maps.[87] Shockingly reported by a jurisdiction (details omitted by the FATF) was a case whereby fraudsters sent emails threatening to not only reveal personal information of victims, but to further infect them and their families with COVID-19 if they failed to pay the fraudsters. [88] Regrettably, South Africa is not excluded from this tragedy as the country struggles with digital fraud such as debit card fraud, phishing, identity theft, third party seller scams, accounts that have been taken over, stolen credit cards or fraudulent charges.

Schemes Related to the COVID-19 Pandemic', available at https://www.fbi.gov/news/pressrel/press-releases/fbi-anticipates-rise-in-business-email-compromise-schemes-related-to-the-covid-19-pandemic (visited 16 June 2022).

83 FATF (May 2020) at 7.

84 Kaspersky (December 2021) 'What is Ransomware?', available at https://www.kaspersky.com/resource-center/threats/ransomware (visited 16 June 2022).

85 FATF (May 2020) at 7. See also Interpol (4 April 2020) 'Cybercriminals targeting critical healthcare institutions with ransomware', available at https://www.interpol.int/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware (visited 16 June 2022).

86 FATF (December 2020) at 10.

87 Ibid.

88 FATF (December 2020) at 10.

3.3 Challenges in the financial sector

Further reported is an increase in online banking, with the inclusion of consumer on-boarding processes and identity authentication. The increasing trend in online banking is reportedly due to limited in-person services, a decrease in opening hours and the actual closure of physical branches of some banks.[89] As elucidated by some supervisors, banks can delay some aspects of customer identity authentication during confinement periods in accordance with a risk-based approach, however, some financial institutions may not be capable of remotely authenticating the identity of customers as noted by FATF and FSRB members.[90] There are continued difficulties in this regard especially for identification purposes associated with financial institutions. With the increase in remote working and online transactions, there has been modification in the financial patterns and behaviours of customers.[91] Reporting organisations might not hitherto be familiar with enabling transactions or conducting services remotely in countries where remote transactions and services are used less frequently which makes customer due diligence or ongoing monitoring increasingly challenging.[92] Compliance staff, in some instances, are still incapable of performing their duties with the same efficacy carried out prior to the COVID-19 pandemic due to remote working and the consequential repercussions on the systems and controls of reporting organisations.[93]

FATF and FSRB members report that as with previous prolonged economic depressions, individuals or organisations in need of funding might approach non-traditional or unlicensed lenders, conceivably including illegitimate groups.[94] Members have also identified the hazard of established financial protectors possibly becoming pre-occupied and distracted with business continuity matters whilst additionally having to see to the surveillance of apprehensive dealings.[95] Risk indicators are required to frequently update and adjust in line with the embryonic risk landscape.[96] Due to the frequent changes over time, communiqué amongst the public and private sectors should be continuous in order to share information.[97] Individuals continue to use unregulated financial services as well as fraudulent schemes that are attractive to those who might have suffered a loss in income or who have lost their jobs. Some are also possibly being misused as money mules.[98] Particular sections of populations such as indigenous or remote societies, the elderly or low-income groups may have an increased risk regarding fraud as they are said to possibly be unfamiliar with online banking

89 FATF (May 2020) at 8.
90 Ibid.
91 FATF (December 2020) at 18 and 19.
92 Ibid.
93 Ibid.
94 FATF (May 2020) at 9.
95 Ibid.
96 FATF (December 2020) at 19.
97 Ibid.
98 FATF (December 2020) at 20.

systems.[99] According to various reports, online bank fraudsters also seek to obtain account or financial data.[100] Since customers' social distancing measures and behavioural fluctuations result in reduced face-to-face interaction, the adequate use of technology, whether used to safeguard effective information distribution between competent authorities and reporting entities or to support the on-boarding process, has become increasingly crucial.[101] South Africa can relate to these findings because it is evident that fraudulent activities have seeped into various businesses, agencies, state institutions as well as departments. These findings also tie in with South Africa's digital fraud, compliance irregularity, lockdown fraud, and maladministration discoveries.

3.4 Misuse of stimulus measures

The global misuse of stimulus measures during the COVID-19 pandemic has not escaped South Africa. According to the report of FATF and FSRB members, a small amount of financial aid focused on individuals and businesses may present possible fraud risks causing ML. More specifically, impostors may deceitfully insist that they offer access to financial aid in order to gain personal financial details.[102] By pretending to be valid businesses in search of aid, FATF members report that offenders might make use of legal entities to falsely claim for government stimulus funding. FATF members advise distributing relief to businesses and individuals through standing government accounts for obtaining social aid.[103] It is said that loan schemes in connection with financial aid are possibly also exploited by criminals for ML.[104] The FATF identified that the exploitation of economic stimulus measures has continued to develop as countries have implemented augmented numbers as well as enlarged sizes of stimulus initiatives.[105] Criminals have indeed been opportunistic in this regard in that individuals, companies, or organised criminal organisations try to deceitfully seek money from governments.[106]

99 FATF (May 2020) at 8. Cellule de Renseignement Financier Luxembourg (2020) "ML/TF Vertical Risk Assessment: Virtual Asset Service Providers" at 1 – 4.

100 FATF (May 2020) at 8. See also Cellule de Renseignement Financier Luxembourg (2020) at 2 and 4.

101 FATF (December 2020) at 19.

102 FATF (May 2020) at 9. See also US IRS (2 April 2020) 'IRS Issues Warning about Coronavirus-Related Scams; Watch Out For Schemes Tied to Economic Impact Payments', available at https://www.irs.gov/newsroom/irs-issues-warning-about-coronavirus-related-scams-watch-out-for-schemes-tied-to-economic-impact-payments (visited 16 June 2022).

103 FATF (May 2020) at 9. Australian Ministers for the Department of Social Services (15 March 2020) 'Youth Homelessness in Australia', available at https://ministers.dss.gov.au/media-releases/5636 (visited 16 June 2022).

104 FATF (May 2020) at 9.

105 FATF (December 2020) at 14.

106 Ibid.

Over and above this, numerous jurisdictions have also articulated apprehensions regarding the probable misuse of international assistance received for fighting COVID-19.[107] In addition, many jurisdictions reported instances of exploitation connected to the mismanagement of government funds initially envisioned for publicly funded contracts or for the usage of medical equipment.[108] To tackle COVID-19, various nations have an instantaneous necessity for urgent financial support.[109] Global financial establishments report that countries where the rule of law is feeble and the practice of accountability and transparency is weak, present a hazard for emergency funding to be embezzled by dishonest officials.[110] Government contracts involving bulk COVID-19 medical supplies also provoke corruption and the misuse of public financial aid, which may worsen if there is the acuity of reduced financial supervision on government procurement and expenditure, as reported by FSRB members. Moreover, as reported by FSRB members, criminals are said to use fraud or informal methods to gain profitable government contracts by bypassing legitimate procurement processes.[111] These FATF detections interlink with those of South Africa especially with regard to the UIF and TERS fraud that ensued.

3.5 Growth in financial unpredictability

The FATF paper has identified growth in financial unpredictability as alarming because unscrupulous criminals might vary their activities to take advantage of the new vulnerabilities.[112] The findings in South Africa during the COVID-19 pandemic sorely refers to this issue as well. According to the FATF's discoveries, one of the aspects that speak to this problem is the economic slump. Criminals might present illegitimate income into the economic structure by rearranging existing methods of credit and loans and may invest in property or struggling businesses in order to produce cash and hide illegal profits.[113] Criminals can smoke-screen the FATF members' emphasis on the fact that tax circumvention and associated crimes could increase as companies and individuals seek to decrease their fiscal burdens, by the freeing up of illegal cash contained in businesses through corporate insolvency proceedings.[114] The economic slump has also caused the private sector entities to have less resources to battle ML / TF and furthermore has, in emerging countries, caused an increase in subsistence crimes involving, for example, theft, wildlife pilfering and burglary.[115] The world continues to endure economic difficulty as alluded to in the FATF December 2020

107 FATF (December 2020) at 16.
108 Ibid.
109 FATF (May 2020) at 10.
110 FATF (May 2020) at 9.
111 Ibid.
112 Ibid.
113 FATF (May 2020) at 9 and 10.
114 FATF (May 2020) at 10.
115 Ibid.

Paper Update. This is said to result in numerous ML susceptibilities.[116] Funds obtained illegitimately is identified as a hazard because it could be used to abuse suffering businesses or businesses prone to swift variations in demand due to, for example, a take-over or the provision of capital.[117] Predominantly exposed are areas such as industrial cleaning, construction, transportation sectors, real estate, and small and medium enterprises in general.[118]

Further aspects that the FATF identified in their Papers is that South Africa may also be a victim of the increase in impacted predicate offences comprising online child exploitation and human trafficking;[119] insider trading relating to bulk value changes in markets;[120] increase in physical cash dealings concerning bank note withdrawals;[121] and virtual assets involving money mule schemes.[122]

It has been established that the aforementioned risks identified by the FATF, whether directly or indirectly, possibly correlate with the occurrences found in South Africa during the COVID-19 pandemic. In riposte to the challenges faced amid the COVID-19 pandemic, the FATF has demonstrated an array of practical examples and actions that have been or are considered to be taken by jurisdictions across the globe. The FATF has produced revolutionary insight and stratagems for its members. A country such as South Africa, plagued with scars from the apartheid regime, overwhelmed by poverty, unemployment, crime, lack of education, healthcare and basic sanitizing, really cannot afford to bear the massive burden of ML and ML threats. It is thus imperative for South Africa to strengthen cognisance of and collaboration with international AML tools such as the FATF.

4. SOUTH AFRICA'S ANTI-MONEY LAUNDERING FRAMEWORK

The *status quo* in South Africa with regards to its AML regime and whether it has the capacity to combat and curb ML and ML threats in South Africa during a pandemic, has to be scrutinised It is important to ascertain whether the South African legal framework is sufficient to address the challenges in relation to ML and ML threats during a pandemic.

It is submitted that the South African AML framework is deeply comprehensive, sufficient, and powerful enough to combat ML and ML threats during a pandemic. South Africa bestows legislation that criminalises and penalises ML offences. ML is a punishable crime in South

116 FATF (December 2020) at 19.
117 Ibid.
118 Ibid.
119 FATF (May 2020) at 8. See also FATF (December 2020) at 6.
120 FATF (May 2020) at 10. See also FATF (December 2020) at 20.
121 FATF (May 2020) at 10. See also FATF (December 2020) at 19 and 20.
122 FATF (May 2020) at 10. See also FATF (December 2020) at 20.

Africa according to legislation.[123] This is provided for in Prevention of Organised Crime Act (POCA).[124] It is moreover submitted that the law in this regard thus does not need any amendments at this point. South Africa is equipped with a framework that is in place for AML measures to be carried out as prescribed by the Financial Intelligence Centre Act (FICA).[125] The country prohibits terrorist and related activities as stipulated in the Protection of Constitutional Democracy against Terrorism and Related Activities Act (POCDATARA).[126] It also governs all procedures that relate to criminal proceedings in South Africa as set out in the the Criminal Procedure Act (CPA).[127] It provides for whistleblowing legislation as seen in the the Protected Disclosures Act (PDA),[128] the Protection Against Harassment Act (PAHA),[129] and the Companies Act and Regulations (CA).[130] It provides for witness protection legislation specified in the the Witness Protection Act (WPA).[131] The Protection of Personal Information Act (POPIA)[132] safeguards personal information or data. The Constitution provides for, inter alia, transparency regarding procurement processes. The Disaster Management Act (DMA)[133] provides for disaster management. The Companies Act and Regulations[134] (CA) provides for the establishment of social and ethics committees within organisations.

South Africa has additionally established corruption, ML and ML threat fighting bodies, institutions, commissions, and strategies. These include the Public Protector, the Directorate for Priority Crime Investigation, the Asset Forfeiture Unit, the Special Investigating Unit, the Financial Intelligence Centre, the Auditor-General, the Public Service Commission, the Independent Police Investigative Directorate, and the National Anti-Corruption Strategy (NACS) for 2020 to 2030.[135] It is also supported in its fight against ML and ML threats by structures such as the SAPS which is governed by the Constitution and the South African Police Service Act[136] (SAPSA); the National Prosecuting Authority Act (NPA Act)[137] which is governed by the NPA Act; and the Service Charter for Victims of Crime in South Africa. Associated legislation including the Constitutional Court Complementary Act (CCCA),[138] the Supreme

123 A detailed discussion of the South African anti money laundering legal framework is outside the scope of this article. For a detailed analysis of the legal framework see Wesso's LLM thesis.
124 Act 121 of 1998.
125 Act 38 of 2001.
126 Act 33 of 2004. See also Hamman & Koen (2012) at 72.
127 Act 57 of 1977.
128 Act 26 of 2000.
129 Act 17 of 2011.
130 Act 71 of 2008.
131 Act 112 of 1998.
132 Act 4 of 2013.
133 Act 57 of 2002.
134 Act 71 of 2008.
135 NACS Republic of South Africa "National Anti-Corruption Strategy (2020-2030)".
136 Act 68 of 1995.
137 Act 32 of 1998.
138 Act 13 of 1995.

Court Act (SCA),[139] the Magistrates' Courts Act (MCA),[140] the Small Claims Court Act (SCCA),[141] the Judicial Service Commission Act (JSA)[142] as amended, the Judges Remuneration and Conditions of Employment Act (JRCEA),[143] the Magistrates Act (MA),[144] and the South African Judicial Education Institute (SAJEI) Act[145] assist the South African judicial authority to be well equipped to adjudicate ML and ML threat matters.[146] It is moreover worth reiterating that the legislation including POCA, the CPA and the NPA Act is sufficient for criminalising ML activities, the reporting of crimes, laying the charges, the investigation of offences, the collection of evidence, the presentation of the evidence in court and the eventual successful prosecution, conviction and sentencing of perpetrators.

The South African AML framework, in as far as its regulations, bodies, institutions, commissions and structures, is thus suitably armed and largely adequate to curb and combat the detected ML and ML threats in South Africa during a pandemic. Yes, of course there are improvements that can and will be made with time and as society develops and where need be. This is completely normal. Life in general is a work in progress. An example of an area in urgent need of improvement and updating of legislation is the area pertaining to e-Discovery in South Africa.[147] However, the pertinent point is that ML is criminalised in South Africa. Further to this, the FATF, in its South Africa Mutual Evaluation Report (2021 MER) released on 7 October 2021, found that the "responsibilities of law enforcement and investigative authorities" (Recommendation 30), and the "powers of law enforcement and investigative authorities" (Recommendation 31) are fully compliant where AML in South Africa is concerned.[148]

Another factor to be respected is that those involved, in a bona fide capacity, with the drafting, building and establishment of South Africa's AML framework have truly invested time, hard work, funding, resources, effort, intellect, grit, and dedication into all the associated processes. To illustrate this point, the hard work that goes into the bona fide process of creating and passing a law in South Africa, for example, can be referred to. The law-making process may commence with a Green Paper which is a discussion document drafted by the Ministry or department tasked with the respective issue considered. The

139 Act 59 of 1959.
140 Act 32 of 1944.
141 Act 61 of 1984.
142 Act 9 of 1994.
143 Act 47 of 2001.
144 Act 90 of 1993.
145 Act 14 of 2008.
146 Sec 165(1) and (2) of the Constitution.
147 Hughes K, Stander A & Hooper VA (2015) 'eDiscovery in South Africa and the Challenges it Faces' DOI:10.1109/InfoSec.2015.7435507 at 1 – 8.
148 FATF (2021) at 213 – 216 and 231.

document provides an idea of the general thoughts which inform a particular policy relating to the issue. The process then proceeds to being published for suggestions, comments, or ideas. Following this is the development of what is known as a White Paper which is a broad statement of government policy. It is an even more refined discussion document that is prepared by the applicable department or task team. The relevant parliamentary committees may then suggest amendments or alternative proposals. It is thereafter sent back to the Ministry for further input and discussion whereafter final decisions are carried out.[149] The aforementioned refers to the passing of laws, but what about the challenging processes in regard to establishing institutions, bodies, commissions and other structures? They all indeed require grit, hard work, time, resources, intellect, funding, effort, and dedication. It is therefore clear that parties involved have made countless sacrifices and have worked tirelessly for South Africa to have a well-equipped AML framework in place. The good intentions in all these processes simply cannot be ignored and further to this, as alluded to previously, ML is criminalised in South Africa. It is a punishable crime during a pandemic or not, and there is a largely sufficient AML framework in South Africa to support this and all associated aspects.

5. THE WAY FORWARD

It is unfortunate and sad that globally and in South Africa people have to suffer and endure the mayhem of money launderers whilst the challenges of COVID-19 have to be navigated. It is an illustration that everyone, from ordinary citizens to law enforcement agencies and politicians, should work together in a concerted effort to reduce the crime and not provide opportunities for criminals. It is essential that the appropriate investigating and prosecuting measures should be in place to address possible future dilemmas. These measures should at least prevent or reduce similar occurrences in a possible future pandemic or disaster.

There should be a proficient and wilful attempt not to make so many opportunities available to criminals. Disasters may happen at any given time. These could include mass poverty, violence during xenophobia attacks, flooding, drought, national power outage, shut down, strikes, wage disputes, defective service delivery and political and social unrest or war.[150]

Considering the largely positive review of South Africa's AML framework, begs the following questions. If the South African AML framework is, with reference to its regulations, bodies, commissions, structures, and strategies, largely adequate to curb and combat ML and ML threats in South Africa during the COVID-19 pandemic, why has such massive amounts of ML and ML threats still taken place? What facilitated and essentially gave perpetrators the 'leeway' to carry out ML and ML threats in South Africa during a global pandemic?

149 Parliament of the Republic of South Africa (2022) 'How a Law is Made', available at https://www.parliament.gov.za/how-law-made (visited 4 May 2022).

150 Wesso (2022) at 76.

It is submitted that it could be the implementation of the legislation that is a problem. There should be an improved protection for witnesses to testify, especially for whistleblowers.[151] More resources should be made available for the investigating and prosecuting institutions in South Africa. Their skill level should be enhanced, and a concerted effort should be embarked upon to retain experienced people or to attract experienced people to work in these departments. It is because people are not arrested and prosecuted successfully, that there seems to be a rationalisation that they can get away with crime[152] and that they are entitled to it. Frequent examples of reasoning during the process of rationalisation of crimes are the following: "I am entitled to it, I can get away with it, others do so why can't I?"[153]

In addition to the above, there simply must be the political will to get rid of corruption.[154] If these issues are not attended to, the same atrocities and criminality will be the order of the day during a future pandemic or disaster. Consequently, questions could be validly posed around whether the largely powerful South African AML framework is a massively tragic waste of resources.

6. CONCLUSION

This article has delved into unprecedented occurrences in relation to financial crimes involving ML and ML threats in South Africa during the COVID-19 pandemic. Many people have suffered and died as a result of the global COVID-19 pandemic. The damage to the economy of countries by the raiding of resources by criminals also had a devastating effect on the lives of ordinary citizens. The COVID-19 pandemic global ML threats, the international combating crusade against ML, and the ML threats during the COVID-19 pandemic were also explored. Examples of crime such as fraud, corruption, theft and many more, has indeed plagued South Africa as well as the rest of the world. The various crimes ranged from a boom in the illegal cigarette market, fraud and corruption with irregular PPE procurement, a surge in financial digital crime, crimes associated with sanitising equipment and fraud with the UIF and TERS. The resultant crime of laundering the proceeds of the acquired illicit wealth also occurs as the criminal attempt to clean their ill-gotten gains to enable them to use the proceeds with impunity.

The crimes illustrated in this article should serve as an alarming wake up call for those in power to urgently put measures in place to prevent similar issues occurring in a future pandemic or disaster. There is an urgent need for the upskilling of certain departments dealing with the investigation and prosecution of crime. Successful prosecutions will indeed serve as a deterrent and a warning to those who think that they can get away with crime.

151 Wesso (2022) at 85.
152 Wesso (2022) at 91.
153 Ibid.
154 Wesso (2022) at 103.

Unless criminals or potential ones are made to realise that there will indeed be consequences because of their criminality, the status quo will remain. Unless rationalisation factors are dealt with and eliminated, the problem will persist.

South Africa is faced with an enormous challenge regarding crime. However, there is always hope that the decrease and possible alleviation of ML and ML threats in South Africa is, in fact, possible.