International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 6, Issue 1
January, 2023
Pages: 523-532

Forensic Investigation: The Impact of Money-Laundering During Lockdown in South Africa

M C Marakalala; R J Mokwena

Department of Police Practice, University of South Africa, Pretoria, South Africa

Email: marakmc@unisa.ac.za; mokwerj@unisa.ac.za

http://dx.doi.org/10.47814/ijssrr.v6i1.1061

Abstract

Research shows that money-laundering has increased exponentially in South Africa during the lockdown caused by COVID-19 pandemic. According to the South African Banking Risk Information Centre (SABRIC), fraudulent online banking and transactions resulted in a sharp increase in cybercrime since the beginning of the lockdown in early 2020, resulting in a huge loss to the banking industry in South Africa. While the Financial Intelligence Centre Act, 38 of 2001 regulate financial transactions, it is evident that criminals are making use of advanced technology to their advantage. Money-laundering ranks among the major crimes, not only in South Africa, but world-wide. A purposive sample of banking employees and investigating officers from the South African police and private investigators employed by the four major banks in South Africa were interviewed using various platforms since lockdown prevented face-to-face interviews. The purpose of this article is to highlight the extend of money-laundering during lockdown and its impact in socio-economic factors. A non-probability sampling (purposive sampling) was used in selecting these participants. These included telephone calls and virtual interviews. The results indicate that there is a relationship between remote online banking and the increase in money-laundering as the system allows transactions to take place with limited verification processes. This paper highlights the significance of considering development of prevention mechanisms, capacity development and strategies for both financial institutions as well as law enforcement agencies in South Africa to reduce crime such as money-laundering. The researchers recommend that strategies to increase awareness for bank staff must be harnessed through provision requisite training and to be provided adequate training.

Keywords: *Corruption; Criminal Investigation; Cybercrime; Forensic Investigation; Fraud; Lockdown; Money-Laundering*

1. Introduction

Money laundering is a serious financial crime that is employed by white collar and street-level criminals alike European Commission (2020:np). According to the South African Banking Risk Information Centre (SABRIC), fraudulent online banking and transactions resulted in a sharp increase in cybercrime since the beginning of the Covid-19 pandemic, resulting in a huge loss to the banking industry in South Africa (AIC, 2003).

While the Financial Intelligence Centre Act, 38 of 2001 regulate financial transactions, it is evident that criminals are making use of technology to their advantage. Money-laundering ranks among the major crimes Globally. It's also present major challenges during lockdown resulting in undesirable audit results and high levels of financial crime. Audits conducted by the Auditor General, SIU and Hawks for the period 2019-2020 showed irregular procurement processes and irregular expenditure resulting in an increased in money laundering during lockdown caused by Covid-19 pandemic (Anonymous, 2019:np). Money laundering is the illegal process of making large amounts of money generated by a criminal activity, such as drug trafficking or terrorist funding. Money laundering is a serious financial crime that is employed by white collar and street-level criminals alike.

2. Purpose of the Article

The purpose of this article is to highlight the extend of money-laundering during lockdown and its impact in socio-economic factors.

3. Research Methodology

A qualitative approach empirical designs were followed in this study. Miles, Huberman and Saldana (2014: 11) describe it as a study that covers an array of interpretive techniques and seeks to describe, decode and translate information to get the meaning of a naturally occurring phenomenon in the social world. The designs were appropriate for this article as there was little information in literature that could achieve the objective of this article, namely proper policing of goods piracy which involves preventative and reactive mechanisms.

The researchers used non-probability sampling as ideal and this design to obtain credible data from respondents and the observation of raids. Data was also gathered through individual telephonically semi-structured interviews.

In view of the contextual background above, the empirical investigation followed a qualitative research design. This will help the researchers to unpack money laundering that is based on a real-life problem.

The paper is empirical since it addresses a real-life problem and has also make use of secondary data in the form of a literature review. The information required for this paper has basically be qualitative in nature. Qualitative research usually initiates with the use of document review to collect information. Data was collected from multiple sources, including relevant national and international literature, pertaining to investigation of money laundering.

The sample was purposively selected because the researchers acknowledge the experience of individuals who had the information and knowledge to assist in this research.

Data analysis

The collected data from interviews were transcribed to facilitate the process. It was analysed methodically according to the thematic method by classification into themes, sub-themes and categories. To this effect, Tesch's eight-step data analysis method, as discussed in Creswell (2014: 198), was used. It involved getting a sense of the whole; picking one of the transcribed interviews and reading it carefully; making a list of topics and clustering them; coding and classifying information; making a final decision and alphabetising the codes; assembling same categories; doing a preliminary analysis; and, finally, recording the data.

Ethical considerations

An ethical clearance was obtained from the College of Law at the University of South Africa. In this article, the researchers ensured confidentiality by not disclosing the personal details of the participants. The researchers obtained informed consent from all 77 participants in this article. Participants were breakdown as 10 SIU members, 35 Bank investigator and 32 Hawks members. The participants consented to be interviewed and were not coerced to partake in the article; hence participation was voluntary. All participants were informed that they were permitted to withdraw from the interviews. Participants were not allowed to discuss their individual responses among themselves. The information they provided was kept in a safe place. Participants were not remunerated for participating in the interviews.

4. Discussion

According to Le Khac, Markos, O'Neill, Brabazon, and Kechadi (2011:504), money laundering is the third largest business in the world. Its turnover is estimated at between 500 billion and 1 trillion US dollars annually. Money from criminal activities is laundered to disguise its origin and elevate it to a legitimate status. Money laundering makes crime a worthwhile endeavor for criminals (Mackrell, 1996:47, South Africa, 1996b: 13). According to Choo and Smith (2008: 45) and Financial Action Task Team Guidance (2013a: 28), these criminals:

- Use agents and mules to open bank accounts for them where transaction will be made to launder the money, and/or;
- Use their intermediaries, family and close associates to launder the dirty money on their behalf and they pay them a service fee or bribe.

South Africa is a member of the FATF, an organisation which sets international standards to combat money laundering and terrorism around the world (Tuba, 2012: 103). All member countries are required to conclude international agreements to combat transnational crimes such as terrorism and organised crime.

Money laundering relates to three broad themes:

- New threats and vulnerabilities stemming from COVID-19-related crime and impacts on Money Laundering
- Current impact on AML/CFT efforts by governments and the private sector due to COVID-19.
- Suggested AML/CFT policy responses to support the swift and effective implementation of measures to respond to COVID-19, while managing new risks and vulnerabilities identified, including charitable activity and economic and fiscal stimulus and financial rescue packages for firms and individuals.

4.1. Covid-19-related money laundering and terrorist financing risks

The Financial Intelligence Centre (FIC) published a notice in March 2020 indicating that there will be no relaxation of obligations under the Financial Intelligence Centre Act 2001 (FICA) during the nationwide lockdown (CISA, 2020:np). A robust money-laundering policy ought to form an integral part of any company's compliance program. Business's compliance functions must operate effectively, even if remotely.

Money laundering and terrorist financing risks

As the impact of the COVID-19 pandemic continues, the money laundering risks are likely to become clearer over the coming months. Nevertheless, jurisdictions continue to see some of the vulnerabilities identified earlier in the year by the FATF as a result of the pandemic. Vulnerabilities revolve around changing financial behaviours, in particular a rise in remote transactions, with impacts on financial institutions' ability to detect anomalies. With increasing unemployment, and larger numbers of citizens conducting transactions remotely, there are also risks that vulnerable citizens will be exploited as money mules.

CISA (2020:np) mentioned that other vulnerabilities relate to increased financial volatility caused by the Global economic downturn triggered by confinement measures to curb the spread of COVID-19. These include increased amounts of cash in circulation, and the use of virtual assets. Many jurisdictions have not identified a change in the terrorist financing risks as a result of the pandemic, although some noted potential future vulnerabilities. These relate to the misuse of non-profit organisations and new opportunities in relation to the predicate threat environment.

Changing Financial Behaviours

Changes in customer behaviour are continuing to make it more difficult for financial institutions to identify anomalies. Customers' financial patterns, for example, are changing as they work from home and conduct more online transactions. In some countries, where remote transactions and services are less frequently used, reporting entities may not yet be accustomed to facilitating transactions or offering services remotely. This makes it more difficult for them to conduct effective customer due diligence or ongoing monitoring (Kruger, 2008:18). In some cases, moves to remote working have impacted the effectiveness of reporting entities' systems and controls, with compliance staff unable to carry out their functions with the same efficiency as they would have done before the pandemic.

According to Europol (2020c:np) the effective use of technology, whether used to support on-boarding or to ensure effective information sharing between competent authorities and reporting entities, has become even more important as customers' behaviour changes and social distancing measures mean that face-to-face interaction isn't always possible. The evolving risk landscape also means risk indicators need to be regularly updated and adjusted, and effective ongoing communication between the public and private sectors is needed to share information as the risks change over time.

In South Africa, 'accountable institutions' (for example banks, insurers and law firms) are under an obligation to comply with FICA and must register with the Financial Intelligence Centre (FIC) (Kruger, 2008:31). All institutions (including accountable institutions) are required to report suspicious and unusual transactions to the FIC with dealers in motor vehicles and Krugerrands also being required to report transactions above certain cash thresholds.

Money laundering risks exist in the day-to-day operations of a company. Europol (2020a:np), stated that in light of a global event like the COVID-19 pandemic, new risks evolve with an enhanced need for corporate compliance teams to keep a close eye on business transactions, source of funds and suspicious and unusual transactions. It is evident that organised criminals have sought to take advantage of the global crisis and corporate uncertainty (Europol, 2020c:np).

On 4 May 2020, the Financial Action Task Force (FATF) published a paper setting out challenges, good practices and policy responses to new money laundering and terrorist financing threats

and vulnerabilities arising from the COVID-19 pandemic. The risks that the FATF have identified include:

- Criminals finding ways to bypass customer due diligence measures by exploiting temporary changes in internal controls caused by remote working situations, in order to conceal and launder funds;
- Increased misuse of online financial services and virtual assets to move and conceal illicit funds;
- Exploiting economic stimulus measures and insolvency schemes as a means for individuals and corporations to conceal and launder illicit proceeds;
- Misuse and misappropriation of domestic and international financial aid and emergency funding by avoiding standard procurement procedures, resulting in increased corruption and consequent money laundering risks;
- Increased use of the unregulated financial sector as individuals move money out of the banking system due to financial instability, creating additional opportunities for criminals to launder illicit funds;
- Criminals exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries, to launder proceeds of unlawful activities, fund their operations, or fraudulently claim to be charities to raise funds online (Europol, 2020c:np).

4.2. The impact of Covid-19 pandemic in money laundering

Covid-19 has not fundamentally altered the predicate offenses for money laundering. Fraud is still fraud. Theft is still theft (Kruger, 2008:65). Yet scam methodologies and money laundering typologies have changed. In this way, Coronavirus could prove to be a catalyst for change in the way regulated entities fight financial crime.

The Coronavirus has been tough for drug traffickers. Global lockdowns closed borders, ports and airports, making it harder for smugglers to move drugs. Criminals also rely on legal trade to camouflage their illegal activities, so as global shipments slowed, drug and cash seizures increased, particularly during the early part of the pandemic.

With business-as-usual disrupted, drug traffickers had to pivot. They had to find new transportation routes as well as ways to clean their dirty cash. This included new overland routes and new cash-intensive businesses and money mule networks as traditional black-market peso exchanges were at a standstill.

With business-as-usual disrupted, drug traffickers had to pivot find new transportation routes as well as ways to clean their dirty cash.

Money laundering will always be needed

While the contribution of particular predicate offenses to overall levels of criminality may change, Covid-19 has not fundamentally changed the nature of predicate offenses themselves (UN, 2020:np). And money laundering still fulfils a fundamental need. Criminals must launder their criminal proceeds so they appear legitimate and can be enjoyed without fear of detection or confiscation.

Financially motivated crime is pointless without a pay-out. This is precisely the point for financial services professionals. Criminals are abusing the infrastructure of the legitimate economy, whether that is bank accounts, credit cards, shell companies or real estate purchases, to make their illegitimate activity pay (Mbaku, 2010:27). Acquirers and those providing payment acceptance facilities to merchants are at risk from and through their merchants (Council of Europe 2020:np).

Unscrupulous merchants may apply for a payment acceptance account and use it dishonestly to cheat their acquirer or introduce risk to the system. Merchants may also act collusively to allow someone else to commit an attack, for example acting as a shell or front company for another entity or allowing their merchant account to be used in a trade-based money laundering scam. Attacks by unknown third parties on acquirers or their merchants are also a possibility (Mbaku, 2010:34).

Covid-19 has not fundamentally changed the nature of predicate offenses themselves - money laundering still fulfils a fundamental need.

It's time to change

Thirty years on from the first set of FATF Recommendations, the global context for money laundering is different (Newburn, 2008:21). Coronavirus has changed it still further in a potentially significant way. Increased public borrowing, rising unemployment, falling economic output, negative growth rates and the very real, human consequences of this perfect storm could bring about a renewed focus on financial crime.

The ‘follow the money’ principle still applies when national and personal finances are spread thin, perhaps even more so. Banks, financial institutions and others in the regulated sector are handling the money that makes the world go around at a time when there is less to go around (Newburn, 2008:11). They could well find themselves under increased scrutiny over their record on, and approach to, dirty money.

Those in the regulated sector must develop the breadth and depth of their capabilities to counter money laundering and terrorist financing threats. To do so, they need to extend their reach beyond their own organization and systems to the digital environment where partners, suppliers, customers and criminals are active (Kruger, 2008:87).

After all, if organizations keep doing what they have always done, they will keep getting what they have always gotten. That may not be enough to protect their business, reputation and bottom line in

the face of changes in regulation, technology and public sentiment around money laundering. It's time to change.

4.3. Money laundering policies at South Africa

Newburn (2008:55) stated that money laundering in the Republic of South Africa is a hot spot for money laundering related activities, including the narcotics trade, smuggling, human trafficking, and diamond dealings. South Africa's position as the major financial center in the region, its relatively sophisticated banking and financial sector, and its large cash-based market, all make it a very attractive target for transnational and domestic crime syndicates. Singapore Police Force (2020:np) stated that the South African Government (SAG) estimates that between $2 and $8 billion is laundered each year through South African financial institutions. The Proceeds of Crime Act (No. 76 of 1996) criminalizes money laundering for all serious crimes. This Act was supplemented by the Prevention of Organized Crime Act (no. 121 of 1998), which confirms the criminal character of money laundering, mandates the reporting of suspicious transactions, and provides a "safe harbor" for good faith compliance. Violation of this act carries a fine of up to rand 100 million or imprisonment for up to 30 years.

The Financial Intelligence Centre (FIC) was established in 2001 to act as the primary authority over Anti-Money Laundering (AML) efforts in South Africa. The FIC is responsible for establishing an AML regime and maintaining the integrity of the South African financial system by enforcing recordkeeping and reporting procedures of financial institutions within the country.

The FIC Amendment Act (No. 11 of 2008) was issued in August 2008 and took effect in 2010 and clarified the roles and responsibilities of supervisory bodies. The Money Laundering and Terrorist Financing Control regulations were published in 2002 and have since been amended on various occasions; they create a comprehensive legal framework for the combating of money laundering and terrorist financing.

AML Training in South Africa

The Proceeds of Crime Act and the Prevention of Organized Crime Act require South African financial institutions to create training programs to combat illicit financial transactions from occurring in the country.

The Economy of South Africa

South Africa is considered an emerging market with an abundant supply of natural resources and well-developed financial, legal, communications, energy, and transport sectors. The South African stock exchange, the Johannesburg Stock Exchange (JSE) is ranked 17th largest in the world (Anonymous, 2018:np).

Throughout history, South Africa has played an important role in trade. Cape Town was established in 1652 by Dutch traders and saw much activity in the centuries to follow, particularly with the discovery of diamonds and gold attracting foreigners to the country. However, economic problems exist from the apartheid era, including poverty, a shortage of public transportation, and general lack of economic empowerment among disadvantaged groups.

Banking in South Africa

The South African Reserve Bank is the Central Bank of the Republic of South Africa. The Central Bank is responsible for the country's monetary policy, as well as bank regulation and supervision in South Africa.

The Reserve Bank also has the sole right to print, issue, and destroy banknotes and coins in South Africa. It issues all new currency through its subsidiaries the SA Mint Company mints all of the country's coins while the SA Bank Note Company prints all of the country's banknotes.

These threats and vulnerabilities represent emerging money laundering (ML) and terrorist financing (TF) risks. Such risks could result in:

- Criminals finding ways to bypass customer due diligence measures.
- Increased misuse of online financial services and virtual assets to move and conceal illicit funds.
- Exploiting economic stimulus measures and insolvency schemes as a means for natural and legal persons to conceal and launder illicit proceeds.
- Increased use of the unregulated financial sector, creating additional opportunities for criminals to launder illicit funds.
- Misuse and misappropriation of domestic and international financial aid and emergency funding.
- Criminals and terrorists exploiting COVID-19 and the associated economic downturn to move into new cash-intensive and high-liquidity lines of business in developing countries.

Interpol (2020c:np), mentioned that AML/CFT policy responses can help support the swift and effective implementation of measures to respond to COVID-19, while managing new risks and vulnerabilities. These include:

- Domestic coordination to assess the impact of COVID-19 on AML/CFT risks and systems;
- Strengthened communication with the private sector;
- Encouraging the full use of a risk-based approach to customer due diligence;
- Supporting electronic and digital payment options.

The participants were asked their view on the extend of money-laundering during lockdown and its impact in socio-economic factors and they all agree that during covid 19 lockdown g in South Africa socio-economic and money laundering has increased significantly. As such, this have negative impact in the social wellbeing of south African society, especially the marginalized group.

Recommendations

The purpose of this research paper is to generate new knowledge with the purpose of empowering forensic investigators who investigate money laundering. The researchers are of the view that amongst others, forensic investigators and external money laundering investigators can achieve this by gathering the relevant knowledge which includes necessary training in the investigation of money laundering.

Findings

The following findings were prepared regarding other relevant points that the researchers came upon during the research:

- Historical perspective of money laundering;
- Conceptualisation of money laundering;
- Perpetrator in money laundering;
- Theoretical explanation of the factors contributing to money laundering;
- The impact of Covid-19 pandemic in money laundering;
- Money laundering policies at South Africa.

The increase in COVID-19-related crimes, such as fraud, cybercrime, misdirection or exploitation of government funds or international financial assistance, is creating new sources of proceeds for illicit actors (Interpol, 2020a:np). Measures to contain COVID-19 are impacting on the criminal economy and changing criminal behaviour so that profit-driven criminals may move to other forms of illegal conduct.

The COVID-19 pandemic is also impacting government and private sectors' abilities to implement anti-money laundering and counter terrorist financing (AML/CFT) obligations from supervision, regulation and policy reform to suspicious transaction reporting and international cooperation.

Conclusion

The impacts of the pandemic continue to evolve. Consequently, the changes in both money laundering and terrorist financing activity as a result of the pandemic are likely to endure to evolve as well. Rising unemployment, financial agony, the bankruptcy of companies, the increased circulation of cash in economies, potential stockpiling of cash by organised criminal groups, and the accelerated implementation of stimulus programs represent vulnerabilities that criminals may increasingly exploit over the coming months. Furthermore, as the development of new COVID-19 vaccines accelerate, so too will opportunities for criminals to devise criminal scams to exploit and illegally profit from these new medical advancements (Interpol, 2020b:np).

The findings of this research reaffirm the pronouncement of money laundering that the core-function of the forensic investigator to conduct the proactive rather than reactive.

This paper concludes that the forensic investigation activities should be measured comprehensively. Law enforcement must be proactive to avoid crime activities.

This paper highlights the significance of considering development of prevention mechanisms, capacity development and strategies for both financial institutions as well as law enforcement agencies in South Africa to reduce crime such as money-laundering. The researchers recommend that strategies to increase awareness for bank staff.

References

AIC, 2003. *Crime reduction matters*. Canberra: Australian Government Printer.

Anonymous, 2018. Komorant. IT Mogul holds computer system 'ransom'. Available at https://kormorant.co.za/42914/mogul-holds-madibengs-computer-system-ransom/(Accessed on 10 July 2019)

Anonymous, 2019. Property 24. R100-million tender fraud alleged. Available at https://www.property24.com/articles/r100-million-tender-fraud-alleged/13278 (Accessed 10 July 2019)

CISA (2020), COVID-19 Exploited By Malicious Cyber Actors, http://www.uscert.gov/ncas/alerts/aa20-099a. (Accessed 10 July 2019)

Council of Europe (2020), In Time of Emergency the Rights and Safety of Trafficking Victims Must be Respected and Protected, https://rm.coe.int/greta-statement-covid19-en. (Accessed 10 July 2019)

Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. (4th Edition). Thousand Oaks: Sage.

European Commission (2020), Launches Enquiry into Fake COVID-19 Related Products, https://ec.europa.eu/anti-fraud/media-corner/news/20-03-2020/olaf-olaf-launches-enquiryfake-covid-19-related-products_en. (Accessed 10 July 2019)

Europol (2020a), COVID-19: Fraud, http://www.europol.europa.eu/covid-19/covid-19-fraud. (Accessed 10 July 2019)

Europol (2020b), How Criminals Profit From The COVID-19 Pandemic., https://www.europol.europa.eu/newsroom/news/how-criminals-profit-covid-19-pandemic. (Accessed 10 July 2019)

Europol (2020c), Catching the Virus: Cybercrime, Disinformation and the COVID-19 Pandemic., https://www.europol.europa.eu/sites/default/files/documents/catching_the_virus_cybercrime_disinformation_and_the_covid-19_pandemic_0.pdf. (Accessed 10 July 2019)

Financial Action Task Team Guidance, 2013. *Money laundering and terrorist financing through trade in diamonds*. Paris: Edmont group of financial intelligence units.

Interpol (2020a), Cybercriminals Targeting Critical Healthcare Institutions with Ransomware., https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2020/Cybercriminalstargeting-critical-healthcare-institutions-with-ransomware. (Accessed 10 July 2019)

Interpol (2020b), INTERPOL Warns of Financial Fraud Linked to COVID-19. [online], http://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraudlinked-to-COVID-19. (Accessed 10 July 2019)

Interpol (2020c), Unmasked – International Covid-19 fraud exposed. [online] Available at: https://www.interpol.int/News-and-Events/News/2020/Unmasked-International-COVID-19-fraud-exposed. (Accessed 10 July 2019)

Kruger, A. 2008. *Organised crime and proceeds of crime law in South Africa*, Durban: LexisNexis, 2008.

Mbaku, JM. 2010. *Corruption in Africa*, Plymouth: Rowman & Littlefield Publishers.

Newburn, T. 2008. *Handbook for policing*. 2nd edition. London: Willan.

Singapore Police Force (2020), New type of e-commerce scams involving the sale of face masks, http://www.police.gov.sg/mediaroom/news/20200222_others_new_type_of_ecommerce_scams_involving_the_sale_of_face_masks. (Accessed 10 July 2019)

UN (2020), Secretary-General's Remarks to the Security Council on the COVID_19 Pandemic, https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-thesecurity-council-the-covid-19-pandemic-delivered. (Accessed 10 July 2019)

Copyrights