A paper presented at the 17th International Conference on Sustainable Development at the Autonomous University, Barcelona, Spain, 2023.

Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud

Mokopane Charles Marakalala
College of Law, School of Criminal Justice
Department of Police Practice, University of South Africa, Preller Street Muckleneuk Ridge, Pretoria, South Africa
Corresponding author: marakmc@unisa.ac.za

OIDA International Journal of Sustainable Development,
Ontario International Development Agency, Canada.
ISSN 1923-6654 (print) ISSN 1923-6662 (online) www.oidaijsd.com
Also available at http://www.ssrn.com/link/OIDA-Intl-Journal-Sustainable-Dev.html

Abstract. This paper focuses on the effectiveness of biometric-based solution to combat Mobile Fraud at the South African Risk Information Centre. SABRIC had the challenges of a successful mobile fraud, cybercriminals could hijack a mobile device and use it to gain access to sensitive personal data and accounts (Anonymous, 2021:np). The cybercriminals are constantly looting the depths of cyberspace in search of victims to attack. Millions of people worldwide use online banking to do their regular bank-related transactions quickly and conveniently. This was supported by the SABRIC who regularly highlighted incidents of mobile fraud, corruption, and maladministration in SABRIC resulting in a lack of secure their banking online, they are vulnerable to falling prey to fraud scams such as mobile fraud.
The online banking payment transaction process to discover what vulnerabilities fraudsters exploit via mobile fraud, and then introduce a computer-based security system which has been developed to help combat mobile fraud (Anonymous, 2021:np). The mobile fraud is technically new form of cyber fraud where hackers gain the personal information and does illegal work with persons bank account and credit card numbers. Similarly, the unethical practices or fraud could be likened to economies which go in cycles, and "as booms turns to bust, frauds emerged as big explosion". Mobile fraud in SABRIC, widespread and an increased business risk for government. Mobile fraud continues to be a persistent and dominant threat facing SABRIC.

Keywords: *Mobile fraud; cybercrime; biometric-based solution; combat; forensic investigation*

Background and Introduction

According to research, South Africa is experiencing a rapid rise in mobile fraud. Fraudulent online banking and transactions led to a significant rise in cybercrime, according to the South African Banking Risk Information Centre (SABRIC, 2019:np). The online banking payment transaction process may be used to identify the weaknesses that mobile fraudsters take advantage of before a computer-based security system is implemented to assist stop it. Even if the Financial Intelligence Center Act, 38 of 2001, controls financial transactions, it is clear that criminals are taking advantage of technology. The South African government's efforts to fight mobile fraud have a negative impact on many communities in South Africa.

Mobile fraud has relied on bolstering legislation, establishing statutory investigative authorities, launching public anti-corruption initiatives, and appealing to public opinion. These individuals were chosen using purposeful sampling, a non-probability sampling technique (Albrecht, Holland, Malagueno, Dolan & Tzafrir, 2015:88). Telephone conversations and online interviews were among them (SABRIC, 2019:np). The findings suggest a connection between remote internet banking and the rise in money laundering since the latter is made possible by the system's lax verification procedures for transactions. In order to minimize crime, including money-laundering, this study emphasizes the need of taking into account the establishment of preventative measures, capacity building, and strategies for both financial institutions and law enforcement organizations in South Africa. The study advises harnessing techniques to raise awareness among bank employees through the provision of necessary training and sufficient training (Caulfield & Steckler, 2014:65).

Problem Statement

The massive problem of fraud in South Africa cannot be solved by requiring mobile networks to collect biometric data. Research by the SABRIC for the years 2017–2021 shows that fraud reports of a biometrics–based solution processes, and the SABRIC is pleased to release its first statistics on digital banking crime. Criminals have taken use of digital platforms since the development of technology, as forensic investigators are all too aware of (Anonymous, 2022:np). In 2017, 13 438 instances involving banking apps, internet banking, and mobile banking caused the sector to suffer gross losses of more than R250,000,000 (Anonymous, 2022:np).

Table 1: The highlights the 4 parties involved in a case of mobile fraud as per the SABRIC's report (2021:np).

Allegation	**Type of Mobile Fraud**	**Year**	**Amount**
Incidents	SIM-Swop fraud	2017/2021	R13,438,00
Loss	Mobile banking fraud	2017/2021	R250,000,000
SIM Swap incidents	Banking apps fraud	2017/2021	
Allegation	**Type of Mobile Fraud**	**Year**	**Percentage**
Mobile fraud Percentages	Debit card fraud	2017/2021	22%

Source: (SABRIC Report, 2021:np)

The final three parties are forced to point fingers at one another while the fraudster makes off with the money. They refuse to take accountability for their role in the con artist's success in the scheme they were duped into falling for. The best precautions should be taken to secure your personal information whether you use online banking or the Internet in general. Anonymous (2020:np) claims that banks frequently inform their customers that they would never send them an SMS or email asking them to click on a link that will connect them to a website where they must update or confirm their online banking information. There are individuals who continue to slip into a despite these warnings (Cieslewicz, 2012:32).

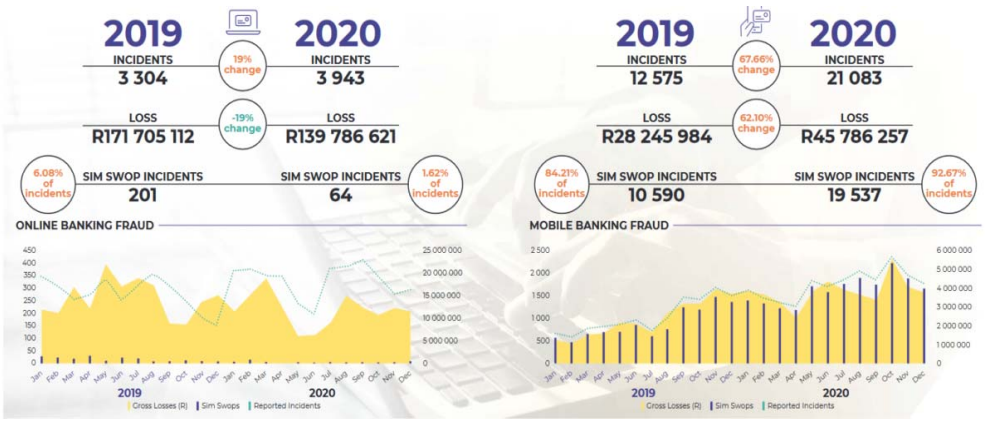


Figure 1: Irregularities of a biometrics-based solution to combat Mobile fraud (Online banking and mobile banking) at South African Banking Risk Information Centre

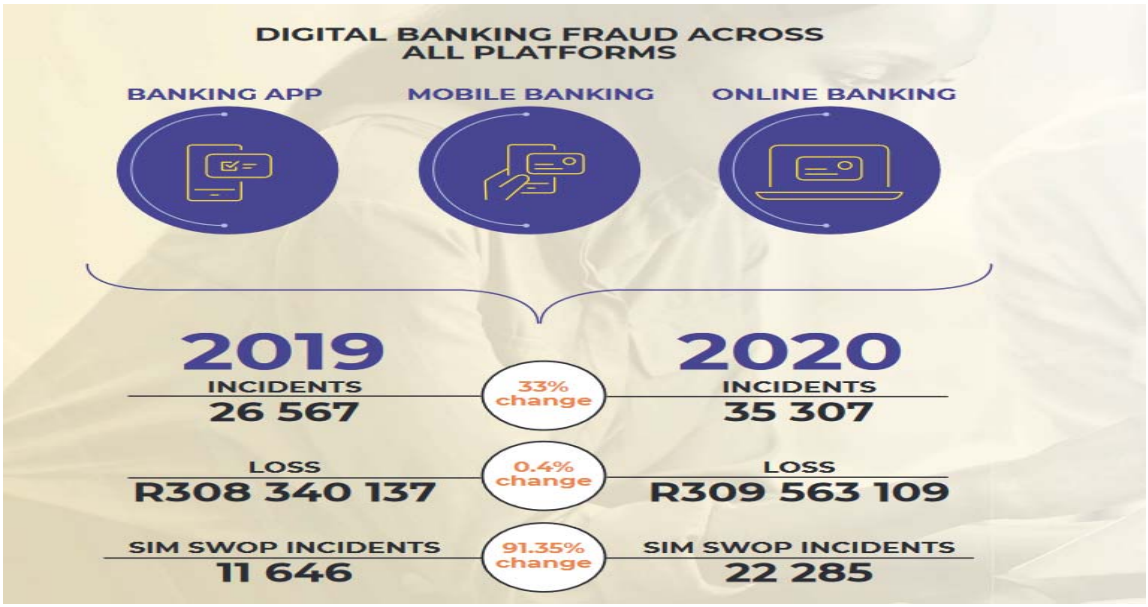
Source: (SABRIC Report, 2021:np)

SABRIC highlighted that although fraud on the internet channel only accounts for 11.1 percent of reported occurrences of digital banking crime, it accounts for the biggest percentage (45.1 percent) of gross losses. By sending the victim to a "spoofed" website that is made to look real, phishing uses emails to fool the victim into entering their login credentials (Anonymous, 2019:np). Vishing, which has been said to have greatly grown in 2020, entails crooks calling potential victims on the phone and enticing them to compromise their details by pretending to be from the bank.

Vishing is sometimes employed by criminals once they have gained access to the victim's account as an extra step to trick the victim into giving them the verification. SIM swaps were reported in 92.7% (19,537) of Mobile Banking fraud incidents reported in 2020 and are the most commonly used combat for committing a crime on this channel, said SABRIC. The increased ability of criminals to carry out SIM swaps may account for the significant increase in incidents (67.6%) and gross losses (62.1%).

Another often reported biometric-based solution on the Mobile Banking channel in 2020 was known party or "friendly" fraud. In this sort of fraud, a person who is familiar to the victim and who is in close proximity to the victim and/or their device (such as a family member or work colleague) is able to access the device and execute transactions on the Mobile Banking platform without the victim's awareness (Bolton, 2016:75). Purchasing airtime or power and using rapid cash sending services are the typical components of this MO's cash-out strategy (Anonymous, 2021:np).

Fraud in online banking surged by 33%. The majority of crimes on this platform are committed through social engineering (phishing, vishing, and SMis SIM swaps), which was recorded in 92.7 percent (19,537) of mobile banking fraud instances reported in 2020. For example, the credentials were saved elsewhere on the device, or the same username and password were used across multiple apps. An increase in the number of incidents involving SIM swaps was reported in 2020 with 26.11% (2,684) as compared to 8% (855) in 2019 (Anonymous, 2021:np).



1.3.3 Figure 2: Digital Banking fraud across all platforms.

Source: (SABRIC Report, 2021:np)

Debit card fraud rose by 22%, while on a positive note, credit card fraud decreased by 7%. ATM explosive incidents climbed by 20% while overall ATM attacks declined by 9%. An increase in the success rate of occurrences during the year was a notable change. In contrast to 2019, where just 40% of occurrences were successful, more over half (54%) of incidents in 2020 were (Mohamed, 2017:23). Analysis revealed that suspects used additional explosives or several explosions to break into safes. This can be attributable to the efficient observation of ATMs for indications of grinding activity, such as a signal loss, together with quick replies from reaction teams. Despite accounting for 27% of the total losses, the corresponding financial losses fell by 50%, according to SABRIC.

Mobile Fraud-Sim Swaps

SABRIC indicated that social engineering techniques, including phishing- the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers, smishing-the fraudulent practice of sending text messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords or credit card numbers, email hacking and business email compromise, continued to prevail and were the most prominent techniques employed in digital banking fraud (PwC, 2014:np).

Research aim and objectives

(Holloway, and Wheeler, 2013:111 see: Kumar (2014:34) stated that the terms' 'goal', 'purpose', 'objective' and 'aim' were often used interchangeably as synonyms for one another. The research aim describes what the researcher plans to be done, attain, or achieve in his or her study. Thus, the aim of a study indicates the biometrics-based solution to combat mobile fraud, whereas the objectives identify the specific issues that the research pro-poses to; in other words, the steps that need to be taken to achieve the aim of the study. Welman, Kruger and Mitchell (2010:02) further added that the aim of a research study is to analyses the different kinds of research methods used when conducting the research. Taking the above ideas into consideration, the researcher decided that the purpose of the research is:

- This paper aim to explore investigation process of the biometric-based solution to combat mobile fraud.

The research objectives are as follows:

Maxfield and Babbie (2011:19) list five different types of research aim, including inquiry, description, explanation, and empowerment, to help realize this clear vision. According to Depoy and Gitlin (2016: 53), conducting research would be a purposeful, intentional, goal-directed activity done for a specific reason, such as researcher to address a particular question or query, (ii) to address a problem, (iii) to address a particular debate or issue. Denscombe (2012:98) adds that it's common to draw a line between critiquing or analyzing something, researching, creating best practices, and empowering others. Maxfield and Babbie (2011:19) list five different types of research aim, including inquiry, description, explanation, and empowerment, to help realize this clear vision. According to Depoy and Gitlin (2016: 53), conducting research would be a purposeful, intentional, goal-directed activity done for a specific reason, such as researcher to address a particular question or query, (ii) to address a problem, (iii) to address a particular debate or issue. Denscombe (2012:98) adds that it's common to draw a line between critiquing or analyzing something, researching, creating best practices, and empowering others.

The research objectives are as follows:

- To identify contributing factors to mobile fraud;
- To implicate more weight on measuring the best practice to combat mobile fraud.

Key theoretical concepts

Because each subject has its own specialized vocabulary and concepts that are well-known to individuals who are in the field, key theoretical concepts are the concepts that appear frequently throughout the whole research study. These terms and concepts become comprehensible within the framework of the study thanks to the definition of essential concepts (Leedy & Ormrod, 2010:58). The explanation of key ideas is essential because it helps the reader understand the research by placing it in the context of the discipline being examined. The reader becomes knowledgeable about the subject and has a clear understanding of the phenomenon being examined thanks to the contextualization of concepts (Babbie & Mouton, 2012:111; Maree, 2007:15; Kumar, 2011:62). In this study, the following fundamental ideas are explained.

Biometric-based solution- Users' live biological traits (such as their face structures, fingerprints, or typing habits) are measured via biometric-based solutions to validate their identities (Gray, 2014:39). It is simple to understand why these solutions are slowly gaining popularity in the business world. The most effective method for quickly and reliably identifying and verifying people using their distinctive biological traits is biometrics.

Mobile fraud- The OTPs and security messages that the account holder's bank would send to the cell phone number during online banking transactions are obtained by fraudsters by stealing a targeted online banking user's cell phone number through mobile fraud (Girard, 2011:88). Mobile network operators, banks, and cell phone consumers all share a common concern about the rapid rise of mobile fraud.

Fraud- Fraud is the illegal and deliberate fabrication of a falsehood that is detrimental to or potentially detrimental to another. Fraud occurs when someone purposefully uses deception to obtain something illegally or unfairly. Hess and Orthmann, (2013:42) mentioned that the act of fraud can be categorized as either a civil or criminal violation in the majority of states. While obtaining rewards of value is the main reason fraud is perpetrated, it can also happen for the express intent of misleading another person or organization. For instance, depending on the situation, making misleading assertions may be regarded as fraud. Take a look at the following fraud definition to learn more about this idea (PwC, 2014:np).

Davis and Pesch, (2013:87) stated that forensic investigation is a process of inquiry into criminal conduct, a civil matter, or an administrative matter that is an in-depth, meticulous search for the truth using specialized skills, expert knowledge, and scientific methods and techniques (also see Van Rooyen, 2008:77).

Combat- The terms opposed, resist, and withstand are some popular synonyms for conflict, according to Kroll, (2013:54), Even though all of these expressions mean "to put oneself against someone or something," combat stresses the violent or urgent opposition of something. combat sickness

South African Banking Risk Information Centre- The terms opposed, resist, and withstand are some popular synonyms for conflict. Even though all of these expressions mean "to put oneself against someone or something," combat stresses the violent or urgent opposition of something. combat sickness. The four major South African banks established the nonprofit South African Banking Risk Information Centre (SABRIC) to support the banking and cash-in-transit sectors in their fight against organized bank-related crimes (Gray, 2014:19). According to recent data from the South African Banking Risk Information Centre, internet banking fraud will rise 33 percent in 2020 as more individuals go online as a result of the COVID-19 pandemic.

Research Methodology

In view of the contextual background above, the non-empirical investigation followed a qualitative research design. This will help the researcher to learn about money laundering that is based on a real-life problem. The paper is non-empirical since it addresses a real-life problem and will make use of secondary data in the form of a literature review. The information required for this paper will basically be qualitative in nature. Qualitative research usually initiates with the use of document review to collect information. Data will be collected from multiple sources, including relevant national and international literature, pertaining to investigation of mobile fraud.

Documentary sources will be to develop an understanding around the theory of ‘investigation of mobile fraud during lockdown in South Africa’. Closed mobile fraud case files will be conducted and analyses. Obtain the opinion and perceptions of the relevant stakeholders such as SABRIC, Auditor General (AG), Special Investigation Units (SIU), and Hawks.

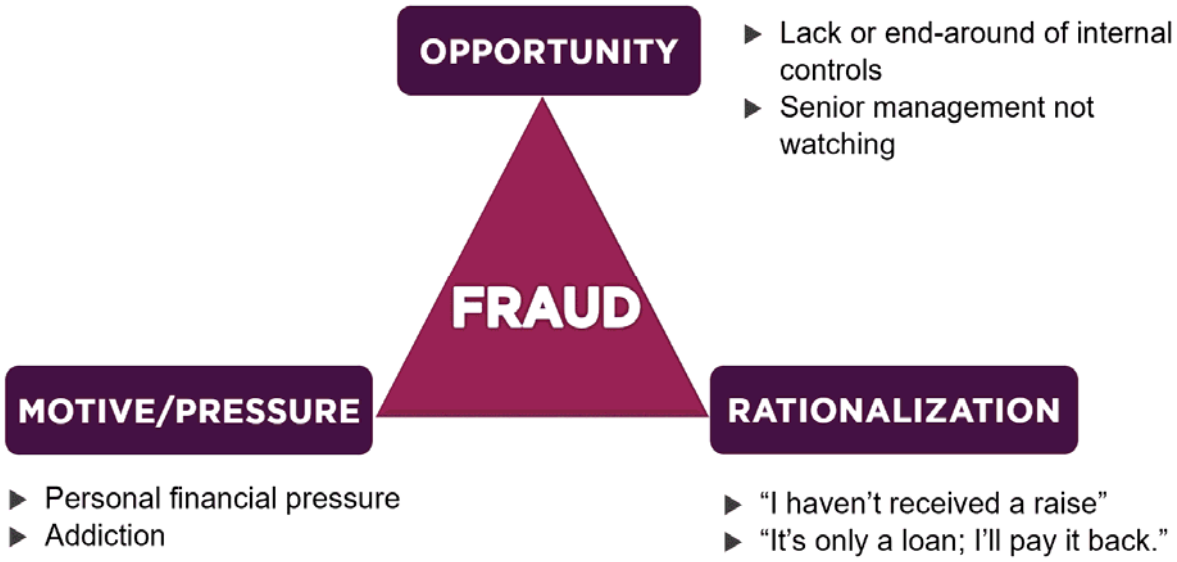
Data Collection

Leedy and Ormrod (2010:12), stated that data collection is the systematic gathering of facts and figures. Kumar (2011:164), points out that the selection of a particular research method to data collection depends on the following aspects:

- The types of information collected;
- The purpose of data collection;
- The resources available;
- The skills and techniques of a particular method to collect data.

Result Analysis and Discussion

Mobile fraud in SABRIC, widespread and an increased business risk for government. Mobile fraud continues to be a persistent and dominant threat facing SABRIC. Fraud studies include information technology, forensics, psychology, accounting, auditing, and management (Lokanan, 2015:76),



Lokanan (2015:74)

To identify contributing factors to mobile fraud

Fraud studies include information technology, forensics, psychology, accounting, auditing, and management. The emergence and increase of fraud may be explained by a model that includes three primary factors: personal pressure, availability of opportunity, and justification of the act or attitude (Wells, 2015:67). Factors contributing to mobile fraud entail the following: non standardized processes i.e. failure to abide to CBK, poor compliance monitoring, interbank competition leading to reduced compliance checks, information sharing hence reduced confidentiality, organization culture i.e. some societies are generally lenient to fraudsters, high cost of transactions hence system abuse, poor remuneration hence staffs handling cash will be tempted to steal, weak pricing policy, maturity of the mobile money services, poor awareness i.e. lack of training and frequent communication, seasonality-fraud is high during festivity, certainty, celebrity, severity, pressure, unemployment, and lack of centralized database for fraudsters (Brytting, Minogue & Morino, 2019:).

Key mobile money risk factors and corresponding indicators include the following:

Product Risk. While the speed, portability, and security of mobile money make it a preferred service in emerging markets, the same qualities make it a preferred channel for more and rapidly executed frauds and scams (James, & Nordby, 2018:91). The emergence of new MFS, including bulk payments, insurance, mobile savings and credit, prepaid cards, and cross-border and international money transfer services, can create opportunities for fraud.

Channel Risk. This risk arises from the ubiquity of mobile phones and the extent to which new and less experienced consumers are entering the market through this channel.

Agent Risk. Providers with large agent networks find it challenging to build adequate infrastructure and systems for effective agent oversight and monitoring of compliance violations, especially in remote areas.

Customer and Compliance Risk. Countries with large numbers of unbanked, illiterate, and/or rural populations that lack national identification regimes find it difficult to ensure know your customer (KYC) due diligence and to track criminal activity, especially given that frontline KYC checks often rely on agents rather than branch staff.

Identity theft arising from fraudulent/offline SIM swaps that transfer the mobile wallet account from the customer's SIM to the fraudster's SIM, enabling the fraudster to gain access to the consumer's mobile wallet and bank account.

False promotions, phishing, or social engineering scams, such as fraudsters impersonating providers and advising customers, they won a prize in a promotion and to send money to the fraudster's number to claim the prize.

This comprehensive guide will cover the intricacies of online advertising fraud specifically in mobile channels, follow its evolution alongside the industry's development, featuring:

- Basic fraud terminology;
- Indications and implications of mobile ad fraud;
- Mobile ad fraud evolution;
- Fraudster profile;
- Common fraud methods;
- Current market and main vertical analysis.

Common types of Mobile Scams:

- Subscriber Fraud;
- Stolen Phones;
- Cloning;
- Text Scams;
- One-ring Scams;
- Recorded Message Scams;
- Phone Insurance Scams;
- Ransomware Scams.

Best practice to combat mobile fraud

Implement multi-factor authentication: The first step for banks is to implement a robust multi-factor authentication process during account registration. Whether the consumer is registering for online banking at home, or downloading the mobile banking application, having a robust multi-factor authentication strategy that leverages things such as out-of-band authentication is the critical first step in preventing fraud online.

Implement and use consumer email and text alerts: One of the most effective ways to prevent fraud is also one of the simplest – email or text alerts. Alerts allow a bank to notify consumers in real-time when there has been any unusual activity online or through a mobile device (James, & Nordby, 2018:123).

For example, if an electronic payment has been made online to a never-before-seen payee, the bank can send the consumer a text alert to their phone to confirm that the requested transaction is legitimate.

Text alerts have not only proven to be an effective tool in stopping fraud, but they also offer a positive customer experience that helps banks establish more trust and goodwill with customers.

Implement and use online activity logging and behavioural analysis: Monitoring consumer's online and mobile access to their accounts is a critical component of preventing account takeover. Activity should be tracked to the Device ID or the IP address and monitored for anomalies such as access from foreign countries, access from devices known to be involved in a prior fraud, a high velocity of recent logins, an escalation in bad login attempts and other unusual circumstances. Monitoring online activity is an important component of protecting consumers against online and mobile fraud.

Implement multi-channel fraud and suspicious activity monitoring solutions: A fraud monitoring solution is an important component in protecting against mobile and online fraud. Fraud monitoring platforms have many off-the-shelf capabilities that help banks to prevent, detect and report instances of fraud.

The most critical components that these systems have are:

Enterprise view – The ability to take in multiple sources of data across different channels to get a holistic view of each customer's account and relationship. This includes checks, electronic payments, access to accounts online and access to accounts through mobile devices.

Scores, rules, and alerts – the ability to generate a risk assessment of a customer's account based on business rules or sophisticated analytic scoring models that use profiles and other techniques to find fraud and create alerts. Fraud reporting – the ability to generate business and regulatory reports when fraud does occur so that it can prevented in the future.

Proactively educate consumers and employees: By educating consumers and employees on the latest fraud scams and schemes, banks can help consumers prevent fraud before it starts. For example, banks should help consumers understand common email phishing schemes that are designed to have them unknowingly provide their login credentials or banking details to fraudsters.

Monitor and clean for malware regularly: Bank hackers are routinely able to steal millions of dollars by convincing customers or even bank employees to click on emails or links that download malicious malware onto their computers.

The malware infects the computer and allows the fraudsters to monitor keystrokes, capture emails, capture screens and other valuable information that they later use to steal from the banks. Scanning for and removing malicious malware is a critical component or reducing online fraud.

Use secure access through HTTPS as often as possible: HTTPS is a protocol for secure connections over the Internet that ensures a person is accessing the site they think they are, as well as making sure data is encrypted so it cannot be stolen. By using HTTPS consumers can ensure against 'Man in the Middle' attacks that allow personal or banking data to be stolen.

Manage online credentials wisely: Changing passwords frequently and making those passwords substantially different from old passwords is a simple but effective way to help prevent online and mobile account takeover. Even if information is stolen, changing passwords frequently may limit or even stop the information from being used.

Methods of data analysis

Taroni, Bozza, Biedermann, Garbolino and Aitken (2010:4), state that data analysis is a process of reviewing, cleaning, changing, and categorising or demonstrating data with the goal of understanding the data. Furthermore, to identify patterns, critical events and irregularities, describing events, and highlighting useful information (Maxfield & Babbie, 2013: 112). The process of analysis goes through certain stages common to many approaches (Holloway & wheeler, 2013: 282). After the data collection process, the researcher used the following steps recommended by Creswell (2013:36) in Leedy and Ormrod (2013: 158-159) to analyse the dataThe process of analysis goes through certain stages common to many approaches. After the data collection process, the researcher will use the following:

Organisation: The researcher will divide the data into paragraphs, sentences and keywords. Categories will be identified in relation to relevant themes and key concepts, namely (i) money laundering, (ii) procurement fraud, (iii) investigation, (iv) tender fraud, (v) financial fraud, (vi) maladministration, (vii) analysis and (viii) MO. The researcher will open different folders in word document format and save the documentation in files and folders on a computer.

Perusal: The researcher will read the data several times to get an overview of what the information as a collective entail.

Interpretation: Literature, documents and other data will be examined for relevance to the topic/theme. The researcher will assemble the collection of data and form a clear understanding of the information. The data will be coded by conducting content analysis and searching for specific words from themes to identify ML.

Identification of patterns: The researcher will scrutinise underlying themes, and other patterns that will describe the topic being investigated more accurately than a single piece of information would reveal. The different

data items from the literature will be summarized and recorded. As a result, it is envisaged that themes and patterns in the data will be identified (Brown, & Holloway, 2013:32).

Synthesis: The researcher will combine all separated data to formulate the overview of the study before arriving at conclusions.

Preliminary Literature Review

A research literature review, according to Brown, and Holloway (2013:19) is a systematic, clear, and repeatable approach for locating, assessing, and synthesizing the body of finished and documented work created by researchers, academics, and practitioners. The findings of a research review are based on the pioneering work of academics and researchers. Creswell (2014:28) elaborates on and supports the aforementioned claim by saying that a literature review is a required element of any research report or thesis. Its major goal is to build a connection between the project and the subject by giving background information and context for the investigation (Girard, 2011:76).

The review may include the following:

- Background information that establishes the existence of the problem to be investigated.
- Previous research on the topic or related topics;
- Theory of relevance to the 'why' questions; and
- Research paradigm(s) as a source of ontological and epistemological assumptions.

The researcher will identify research previously conducted on social grant fraud – for example the following:

The importance of a forensic investigation to combat mobile fraud with biometric-based technology at the South African Banking Risk Information Center. Additional suggestions from the study, which was conducted in 2019 at the University of South Africa (Unisa), call for focusing in particular on the methods used to perpetrate fraud in the context of mobile fraud.

According to Michael-Kramer (2012:33), SABRIC should take the following actions as a result of mobile fraud in South Africa, Institute of Security Studies Monograph 154, November 2008, which was one of the primary suggestions.

- Implement a strong internal control mechanism;
- Internal reflection on anti-corruption efforts;
- The above literature will help the researcher to understand what has already been written on the subject, including addressing the gaps.

The researcher will obtain insight into concepts related to the research problem by doing the following:

- Checking South African literature on combat, biometric-based solution, fraud and mobile fraud;
- Checking Google Scholar books, including other online books;
- Checking journal articles;
- Conducting a general search on key concepts on the Internet; and
- Creating alerts from Google on topics of research interest.

Research Findings

The following findings were prepared regarding other relevant points that the researcher 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.

Recommendations

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

Conclusion

The findings of this research reaffirm the pronouncement of mobile fraud that the core-function of the forensic investigator to conduct the crime prevention and to be 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 researcher recommends that strategies to increase awareness for online banking.

References

1. Albrecht, C., Holland, D., Malagueno, R., Dolan, S. and Tzafrir, S. (2015), "The role of power in financial statement fraud schemes", Journal of Business Ethics, Vol. 131 No. 4, pp. 803–813.
2. 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 2023)
3. Anonymous, 2021. Hawks probe SABRIC for gross mobile fraud. Available at https://city-press.news24.com/News/hawks-probe-SABRIC-for-gross-mobile-fraud-20210528 (Accessed 10 April 2022)
4. Anonymous, 2022. Association of Internal Control Practitioners. (2021), "Combatting Mobile fraud", available at: https://www.theaicp.org/combatting-Mobile-fraud/ (Accessed 20 January 2022).
5. Babbie, E. & Mouton, J. 2011. *The practice of social research*. Cape Town: Oxford University Press.
6. Babbie, E. 2012. *The practice of social research.* Belmont: Wadsworth.
7. Bennett, W. W. & Hess, K. M. 2017. *Criminal Investigation.* 8th edition. Belmont: Wadsworth/Thomson Learning
8. Brown, L. & Holloway, I. 2013. *Qualitative Research in Sport and Physical Activity*. SAGE Publications Ltd
9. Brytting, T., Minogue, R. and Morino, V. 2019. The Anatomy of Fraud and Corruption: *Organizational Causes and Remedies,* Gower Publishing, Ltd.
10. Buckles, T. 2017. *Mobile fraud Scene Investigation: Criminalistics and the Law*. New York: Thomson Delmar Learning.
11. Caulfield, T. and Steckler, S. (2014), "*The five faces of Mobile fraud, abuse, and noncompliance*", Contract Management, Vol. December, pp. 38–45.
12. SABRIC Report. (2021), *Deterring and Detecting Financial Reporting Fraud*: A Platform for Action, available at: http://www.thecaq.org/deterring-and-detecting-financial-reporting-fraud (accessed 11 June 2023).
13. Cieslewicz, J. K. (2012), *"The fraud model in international contexts: A call to include societal-level influences in the model"*, Journal of Forensic & Investigative Accounting, Vol. 4 No. 1, pp. 214–254.
14. Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. (4th Edition). Thousand Oaks: Sage.
15. Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. (4th Edition). Thousand Oaks: Sage.
16. Davis, J. S. and Pesch, H. L. (2013), *"Fraud dynamics and controls in organizations",* Accounting, Organizations and Society, Vol. 38 No. 6–7, pp. 469–483.
17. Denscombe, M. 2012. *Research Proposals-A practical guide.* McGraw- Hill House: Open University Press.
18. DePoy, E. & Gitlin, L. N. 2016. *Introduction to Research: Understanding and Applying Multiple Strategies*. (5th Edition). USA: Elsevier
19. Girard, J. E. 2011. Criminalistics: Forensic Science and Mobile fraud. Burlington: Jones and Bartlett.
20. Gray, D. E. 2014. *Doing research in the real world*. London: SAGE.
21. Hess, K. M. & Orthmann, C. H. 2013. *Criminal Investigation*. 10th edition. Mason, OH: Cengage Learning.
22. Holloway, I. and Wheeler, S. 2013. *Qualitative Research in Nursing and Healthcare*. (3rd Edition). UK: Wiley-Blackwell, A John Wiley & Sons, Ltd.
23. James, S. H. & Nordby, J. 2018. Forensic science. *An introduction to Scientific and Investigative Techniques*. 3rd edition. Boca Raton: CRC Press.
24. Kenney & McCafferty, 2016. *False Claims Act. Medical Device Lawsuit*: Settlement. P.C.
25. Kroll. (2013), "2013/14 Global Fraud Report", available at: http://fraud.kroll.com/introduction/ (accessed 21 March 2022).

26. Kroll. (2013), "2013/14 Global Fraud Report", available at: http://fraud.kroll.com/introduction/ (accessed 21 March 2023).
27. Kumar, R. 2011. *Research Methodology- a step-by-step guide for beginners*. (3rd Edition). London: SAGE Publications.
28. Kumar, R. 2014. *Research Methodology. A step-by-step guide for beginners.* (4th ed). London: SAGE.
29. Leedy, P.D. & Ormrod, J.E. 2016. *Practical Research: Planning and Design*. (11th New Jersey): Pearson Education International.
30. Lokanan, M.E. (2015), "*Challenges to the fraud triangle: Questions on its usefulness"*, Accounting Forum, Vol. 39 No. 3, pp. 201–224
31. Mark M. L. and Lisa T. B. 2014. *Research Methods in Crime, Justice, and Social Problems.* 2nd Edition. Oxford University Press
32. Maxfield, M. G. & Babbie, E. 2015. *Research Methods for Criminal Justice and Criminology*. Belmont: Wadsworth.
33. Maxfield, M. G. & Babbie, E. R. 2011. *Research Methods for Criminal Justice and Criminology*. Belmont, CA, Wadsworth Pub.
34. Michael-Kramer, W. 2012. *The most common Mobile fraud schemes and their primary red flags.* Available at https://iacrc.org/procurement-fraud/the-most-common-procurement-fraud-schemes-and-their-primary-red-flags/ (Accessed 14 March 2022).
35. Morrow, S. L. 2005. Quality and Trustworthiness in Qualitative Research in Counselling Psychology. Journal of Counseling Psychology.
36. Noble, H. & Smith, J. 2015. Issues of validity and reliability in qualitative research. Evidence-Based Nursing, 18 (2).
37. PwC. (2014), "Global Mobile fraud Survey 2014", available at: http://www.pwc.com/Mobile fraudsurvey (accessed 21 March 2022).
38. Taroni, F., Bozza, S., Biedermann, A., Garbolino, P. & Aitken, C. 2010. *Data analysis in forensic science. A Bayesian decision perspective.* West Sussex: John Wiley & Sons.
39. Van Graan, J. & Budhram, T. 2015. Principles of Evidence. In Zinn, R.J. & Dintwe, S.I. (eds). 2015. *Forensic Investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta
40. Wells, M. 2015. Mobile fraud. *The key to understanding and mitigating Mobile fraud risks*. Available at: http://www.procurementfraud.co.za/search/our-greedygovernment.php (Accessed on: 7 April 2022).
41. Welman, J.C., Kruger, S.J. and Mitchell, B. 2010. *Research methodology for the business and administrative sciences*. (6th Edition). Johannesburg: Thomson.
42. Welman, J.C., Kruger, S.J. and Mitchell, B. 2010. *Research methodology for the business and administrative sciences*. (6th Edition). Johannesburg: Thomson.
43. Zinn, R.J. & Dintwe, S.I. (eds). 2015. *Forensic investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta.