Dialogues in Humanities and Social Sciences
2025, VOL. 3, NO. 1, 39-46
ISSN (P): 3078-8838 ; ISSN (O): 3078-8846
https://doi.org/10.71261/dhss/3.1.3946

OPEN ACCESS

Forensic Expert: An analysis of the solution in the App Kidnappings Links to Financial Fraud in South Africa Banking Industry

Mokopane Charles Marakalala[1]

[1] University of South Africa, College of Law, School of Criminal Justice, Police Practice Department, South Africa.
Email: Marakmc@unisa.ac.za

ABSTRACT

Research shows forensic experts revealed that as of the 2022/2023 financial year, the total number of kidnappings in South Africa reached 15 343 cases. Gauteng had the highest number of kidnappings, with 7 818 reports. KwaZulu-Natal followed with 3 081 cases of kidnapping in the same period. The escalating number of kidnappings in South Africa has reached unprecedented levels, with recent incidents shedding light on the dire reality faced by citizens. According to Statistics SA (StatsSA), more than 16 000 kidnappings are recorded annually in South Africa. Shockingly, 85% of these victims are women and children. Reasons for the kidnapping range from ransom demands to human trafficking, drugs, business debts, feuds and, in some cases, for muthi (traditional medicine) where human body parts are used. Crime statistics reveal a 183% increase in kidnapping cases over a nine-year period. From the 2012/2013 period, where 3 832 cases were reported, to the 2021/2022 period, where 10 826 cases were recorded, the trend has shown no signs of abating. This study aims to analyses the biometrics technology link app kidnappings to financial fraud in South Africa and Africa. Design/methodology/approach discusses from secondary sources of data, mainly drawn from journal articles, internet sources and scholarly books relevant to leadership and public administration in developing African countries and how the biometrics technology link app kidnappings to financial fraud can be combat crime such as financial fraud to ensure awareness and protection in the society. This will bring about a renewal of thought and practice of public protection on the continent.

ARTICLE HISTORY
Received 02 Jan. 2025
Accepted 19 Jan. 2025
Published 05 Feb. 2025

KEYWORDS
biometrics, technology, link, app, kidnappings, financial, fraud.

Introduction

The introduction of mobile telecommunications and later, the adoption of mobile phones to provide financial services changed the dynamics of the industry, bringing financial services closer to the public through existing merchant infrastructure within local communities (Isa, 2011:678). This study focuses on an exploration of biometric-based solution in combatting mobile fraud in the South Africa Banking Industry (SABI). Kyle (2020:np) postulated that post 2000, South African Banking Risk Information Centre 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. Ezejiofor, Nwakoby & Okoye, (2016:11) added that 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 SABI resulting in a lack of secure their banking online, they are vulnerable to falling prey to fraud scams such as mobile fraud in SABI (Anti-Intimidation and Ethical Practices Forum (AEPF) (2020:np)

Fraud is a critical problem of global concern (Wanemba, 2010:np), It involves the use of occupation for personal benefit via a deliberate misuse or misappropriation of an organization's resources [Association of Certified Fraud Examiners (ACFE), 2012, 2019]. A financial expert has pointed out that the increased use of cellphone-based payments like digital wallets could lead to prolonged hostage situations Ironically due to the additional security measures they provide (UK Finance, 2018:np). The South African Police Service recently revealed that 3,641 kidnapping cases were reported to its stations between April and June 2023. Van Niekerk, B. (2017: 89) indicated that works out to 40 kidnappings per day. Banks in South Africa have increasingly encouraged the adoption of digital payment methods. This includes linking cards on a smartphone or

CONTACT Mokopane Charles Marakalala Marakmc@unisa.ac.za South Africa

smartwatch for contactless (tap) or QR-code payments instead of physical cards or cash (Ramadani, Siahaan, Sutrisno, Amelia, Dalimunthe & Munthe, 2018:201).

These services allow users to link a physical or virtual card to an NFC-enabled smartphone or smartwatch and make payments with that card by tapping phone (Tiwari, Bhalla & Rawat, 2016:19). Aside from making it more convenient to pay by allowing you to leave your wallet in the home or car, these payment methods can also provide extra security as they require that users enable the strongest security features of their devices. The South Africa banking industry is managed and controlled by the South Africa Reserve Bank (SARB) as the regulatory authority over the banking industry and financial institutions, aiming to achieve a robust and efficient banking system in the interest of the customers and the economy in accordance with the Banks Act (No. 94 of 1990), or the Mutual Banks Act (No. 124 of 1993) (SARB, 2020). Information Technology (IT) is critical in achieving this aim and for performing the day-to-day operations for most organisations (Ali, Ali, Surendran & Thomas, 2017:70). However, it can be said that IT has an adverse impact on the banking industry, too, where crimes such as phishing, hacking and forgery are committed (Ramadani *et al.,* 2018:341).

Research Method

According to Mouton (2012:55), a research design is a plan or outline of how one intends to conduct research. A researched design is dependable on the researched problem of the study (Leedy & Ormrod, 2016:26). The researcher's choice of design will be non-empirical in nature. This will help the researcher to learn and understand mobile fraud that is based on a real-life problem and in line with the topic (Maxfield & Babbie, 2011:06; Ary, Cheser, Sorensen & Walker, 2019:65).

The qualitative design was adopted to fulfil the purpose of the study. Bertram and Christiansen (2014:34); Babbie (2021:77). refers to qualitative methodology as those research methods such as documentary analysis or desktop research, total contribution to the activity being examined and field work of data collection, among others, that permit the researcher to obtain first-hand knowledge about the non-empirical social world in question. Aurini, Heath and Howells (2016:65) stated that the advantages of this approach are that the researcher is close to the information, can do a follow-up when something is not clear, and the information is valid.

Bachman & Schutt (2010:54), define qualitative methodology as the research that produces descriptive data, generally the documentary analysis or desktop research pertaining to data collection. Usually, no numbers or counts are assigned to these documentary analysis or docket analysis. Welman, Kurger & Mitchell (2010:41) further write that qualitative methodology allows the researcher to know desktop research normally allows the process of data collection to be productive with real-life situations. This enables the researcher to interpret and describe the actions of documentary analysis or desktop research.

De Vos et al. (2011:65) points out that qualitative researchers tend to collect data in the field at the site where the documentary analysis or desktop research were the issue or problem under study. Researchers collect data themselves by examining documentary analysis or desktop research. They gather multiple forms of data rather than rely on a single data source and they try to develop a complex and holistic view of social phenomena (Bezuidenhout, 2021:88). This study is about the role of an analysis of the solution in the app kidnappings links to financial fraud in South Africa Banking Industry. The qualitative method best suits this study because the researcher conducted non-empirical study where analyses documents or desktop research understand the environment and have experience because of their duties. That means that rich information was collected.

Research design is expected to produce the foundations for a competent and effective research project (Bachman & Schutt, 2010:64; Blaickie 2009:84); Bougie & Sekaran, 2016:55). argues that it is the most challenging part of a research project. Bertram and Christiansen (2014:40) assert that research design is a plan of how the researcher will systematically collect and analyse the data that is needed to answer the research question. The designed and planned nature of observation distinguishes research from other forms of observation (Clark, Foster & Bryman, 2019:18). Research design is the planning of any systematic research from the first to the last step. It is thus obvious that the aim of the research design is to align the search for scientific knowledge with the practical considerations and margins of the project being embarked on at an exploratory level.

The study was non-empirical since it addresses a real-life problem and will make use of secondary data in the form of a literature review. The purpose of this research was to analyses as it describes the situation and suggests or recommends solutions to the problem which was identified (Bolton, 2016:104). Qualitative research methodologies were used to address the research question. The information required for this study was qualitative in nature. Qualitative research usually initiates with the use of document review

to collect information (Creswell, & Creswell, 2018:43). According to Gordhan (2014:26), a qualitative approach is subjective, value laden, biased and inductive rather than deductive. Qualitative research enables the researcher to gain new insights into a phenomenon as well as to evaluate the effectiveness of existing practices (Kathryn, 2017:19; Creswell & Poth, 2018:91). A qualitative research design best suited the aim and purpose of this study, which required the collection of in-depth information to explore and understand the biometric technology to combat mobile fraud in SABI.

Data was collected from multiple sources, including relevant national and international literature, pertaining to the biometric technology to combat mobile fraud of perpetrators. Documentary sources or desktop research was analyses and an understanding around the theory of "an analysis of the solution in the app kidnappings links to financial fraud in South Africa Banking Industry of perpetrators was developed.

Study Population

A population is any set of desktop research from which the sample is selected and to which this study results will be generalised (Marion, 2004:90; David & Thomas, 2018:33; Creswell, 2020:29). Brynard and Hanekom (2006:55) assert that a population refers to desktop research that possesses specific characteristics, for example public officials with post-graduate degrees. The universe refers to all subjects who possess the attributes in which the researcher is interested, for example everyone – the entire number of inhabitants –in the world, who possesses a post-graduate degree.

Bertram and Christiansen (2014:59); DePoy and Gitlin, 2016:90) posit that the word 'population' is used to mean the total number of desktop research in the organisations that could be included in a study. It could also be objects, subjects, phenomena, cases, events and activities that the researcher wishes to research in order to establish new knowledge. According to De Vos *et al.* (2011:223), population is the totality of document files, events, organisation units, case records or other sampling units with which the research problem is concerned. In this study, the population consisted of 35 investigation files from SABI.

In the opinion of Richie and Lewis (2003:86); Bachman and Schutt (2014:106). A researcher must first define the so called "parent population", regardless of the number of units of analysis. This then represents the overall population when a sample must be selected. These authors suggest that three crucial questions must be asked to define the population for a research study (Richie & Lewis, 2003:87; Bachman & Schutt, 2014:112). These questions must flow from the research question which is explained below. If they are not accessed properly, they may have an influence on the eventual outcome of the research. The questions must:

- Confirm whether a certain "group or sub-population is of central interests in the research.
- Due to the prevalence of certain scenarios or experiences, one must establish whether any specific "sub-sets of the population need to be excluded.
- It must also be ascertained whether any additional sub-population needs to be included.

For this qualitative research study, the parent population was identified as the available and relevant 35 investigation files on desktop research that have been finalized by the SABI for the period 2017 to 2022.

Sampling Procedures

A sample on this study refers to desktop research drawn from a population. The goal is to be able to find out true facts about the sample. Bertram and Christiansen (2014:59); Henning (2018:87) mentioned that a sample involves making decisions about which desktop research, settings, events or behaviours to include in the study. Researchers have to decide how desktop research will be observed. De Vos *et al.* (2011:223) define sampling as a means of taking a portion or a smaller number of units of a population as having the characteristics of that total population. The ideal sample of this study was drawn from SABI in the Gauteng Province and the national office.

Sampling refers to the principles and procedures used to identify, choose and gain access to relevant units, which is used for data generation by any method (Mason, 2001:83, Hadi & Closs, 2016:38). The basic principle of sampling is that it is possible to produce accurate findings without the need to collect data from each member of a surveyed 'population' (Denscombe, 2012:23). Bachman and Schutt (2014:108) identified probability and non-probability sampling methodologies, which they argue must be considered when doing research.

Probability sampling refers to when the probability of the chosen population elements had not yet been identified whilst non-probability sampling is a technique in which the researcher selects samples based on the subjective judgment of the researcher rather than random selection. It is a less stringent method (Denscombe, 2012:23; Bachman and Schutt, 2014:108). As part of this research the method of non-

probability sampling was selected and incorporated throughout. Maree (2007:80), Welman, Kurger & Mitchell (2010:56) explains that due to the lack of random selection of population elements, it is advisable to make use of non-probability sampling when conducting research because no action in the form of random selection need to be applied when choosing a researched sample (also see, Lanier & Briggs, 2014:206; Bachman & Schutt, 2014:109; Hennink, Hutter & Bailey, 2020:98)

To get an understanding of the past and current MO types perpetrated into mobile fraud at SABI and determine similarities, if any.

In an alignment with the aim of this research and the research questions as defined, the following fields were identified as crucial from an accuracy and completeness perspective for qualitative research.

Results and Discussion

Banking app kidnappings are on the rise in South Africa Banking Industry: see the case on victims may be detained against their will and coerced into unlocking their mobile devices, granting offenders access to their banking applications (Bankscope, 2018:np). All available funds in the victim's accounts, including credit balances and accessible home loan accounts, are transferred to intermediary mule accounts or withdrawn at various ATMs. Concerningly, several documented incidents have been characterised by high levels of violence. BusinessTech (2017:np): Cassim (2016:91), furthermore, it is worth noting that while the modus operandi is frequently reported in express kidnapping cases, similar methods are observed in some kidnapping-for-ransom situations. In these instances, perpetrators withdraw available funds from the victim's accounts at ATMs, while simultaneously demanding a ransom from the victim's family (Dagada, (2013:np).

A worrying new crime trend has emerged in South Africa: victims are being kidnapped and coerced, often under the threat of violence, into making transfers from their banking apps, often stripping them of all their savings or completely looting their other accounts (Dzomira, 2014:11). Incidents involving kidnapping or hijacking of individuals, with the aim of gaining unauthorised access to their banking apps under duress, are on the rise (Dzomira, 2014:14). Victim's identification and individualisation in mobile fraud cases. Different identification methods relating to specific aspects will be examined and evaluated, including the victim, the perpetrators and the points of compromise and fraudulent spend. Victims' accounts are used to make online purchases both locally and across South Africa's borders (Dlamini & Mbambo, 2019:np).

These "shakedowns" are executed in a number of ways: Some victims are forced to make payments into bank accounts outside of the country, which makes tracing the funds nearly impossible for law enforcement. In other cases, victims' accounts are used to make online purchases both locally and across South Africa's borders (Dzomira, 2014:18). In yet another example, multiple digital wallet payments or account transfers are made to a local recipient by syndicate members holding the victim hostage while other perpetrators drive around and make withdrawals at ATMs as quickly. In all instances, common banking app protection features including Pins, biometric authentication and facial recognition prove to be ineffective (Joyner, 2019:np). "In an app kidnapping where someone is forced to open their own profile on their own phone and there isn't much one can do. It's like someone forcing the victim at gunpoint to withdraw cash using victim's own card and Pin at an ATM" (Dzomira, 2015:09).

Banking app kidnappings – what to do: For many, the knee-jerk reaction to what is perceived as a helpless situation is to delete all banking apps on personal devices entirely, but this makes transacting and managing funds on a day-to-day basis cumbersome. Ndlovu (2023**:**np) indicated that human recommends a workable middle ground: "Keep only enough funds in transactional account to cover immediate expenses. Place the rest in a seven-day (or longer) notice account. If the bank client then need urgent access to it, can action an 'early breakage', but funds will only be available the next day long after the criminals have moved on," This strategy may work for some people, provided their banking needs do not go beyond the simplicity of a transactional or savings account, but it is not applicable in all cases all the time.

As George Wandsella, head of enterprise risk and fraud strategy at TymeBank, explains, banking app shakedown syndicates are discerning in the way they choose their targets, often homing in on individuals more likely to have a sophisticated account profile with more banking products – and more money in those accounts (Ndlovu**,** 2023**:**np). "Kidnapping cases can affect anyone, but generally speaking those higher at risk include children, business owners, high-income individuals, those living alone and newcomers to South Africa," (Ndlovu**,** 2023**:**np). Representatives from Standard Bank, TymeBank and Bank Zero all told TechCentral that detecting and stopping a banking app shakedown in progress is difficult to do. Tracing stolen funds after the fact also often leads nowhere because, although law enforcement may know where the money was withdrawn, finding the perpetrators is difficult because they change their hunting grounds often. For consumers to insulate themselves, they must be aware of how these criminals operate.

Prevention is key for this type of crime, and customers are urged to educate themselves on the tactics used by criminals and ensure that the necessary precautions to prevent kidnapping are exercised (Wandsella, 2023:np). Although an extra dose of vigilance might help stop some incidents, it is no magic elixir. When the worst that can happen does, subject matter expert - Christina Pieterse, head of Nedbank's digital channels, recommends the following protocol for banking app shakedown victims:

- ***Cooperate:*** The safety of victims or client's life should always be top priority. If someone is threatening victims or clients with violence, it's best to cooperate.
- ***Stay calm:*** Try to remain as calm as possible. Panic can escalate the situation, so it's essential to keep a level head.
- ***Memorise details:*** If the victims or clients can, make mental notes about the assailants' appearance, accents, or any identifying features. This information may be helpful to law enforcement later.
- ***Stay passive:*** Avoid any sudden or aggressive actions that could provoke the kidnappers.

***The victim of have to comply with syndicate demands*:** Comply with syndicate instructions, such as accessing your banking apps. The victim's personal safety should always come first.

Seek help later: Once the situation is resolved, immediately contact the authorities and bank to report the incident.

The South African Banking Risk Information Centre (SABRIC) furthermore tracks banking-related criminal activity, providing information on the various types of banking crimes (Modugu & Anyaduba, 2013:189). In its Annual Crime Stats 2022 report released last month SABRIC 2023 noted that other types of mobile banking crimes were in decline while banking app fraud cases increased by 36%, suggesting that criminals are now migrating to banking app shakedowns and other methods since the previously popular Sim-swap method is proving to be less effective than in the past. Encouragingly, the number of reported mobile banking fraud incidents saw a 9% reduction in 2022. Additionally, incidents involving Sim swaps declined from 87% in 2021 to 76% in 2022, indicating a waning efficacy of this fraudulent tactic.

Conclusion

The Southern African Fraud Prevention Services (SAFPS) has reported a rise in fraudulent activities, including a new trend of criminals targeting banking apps to loot victims' bank. In 2019, 84% of child kidnapping cases were facilitated through social media (South African Reserve Bank (SARB), 2020:np). This statistic is a stark reminder of the dangers of social media when it comes to child kidnapping. Digital kidnapping is the theft of a minor's photos, posing as them, or posing as their parents. SABI is commonly done to reveal private or sensitive information that negatively impacts the child's life, making it difficult to gain acceptance to college, or subjecting them to bullying (SABRIC, 2022:np). The results obtained indicated that the impact of cyberfraud on the South African banking industry is significant and that the occurrence of cyberfraud affects the reputation of the South African banking industry in terms of reputation loss, revenue loss, productivity loss and shareholder loss. According to the results obtained, the prevalent forms of cyberfraud perpetrated in the South African banking industry include phishing, spying, malware, data theft, spam e-mail, online theft, hacking and skimming.

This study provides empirical findings that could assist the South African banking industry in the areas decision making or policy formulation geared towards of cyberfraud mitigation. This research notifies the South African banking industry about the nature of cyberfraud perpetrated (South African Banking Risk Information Centre (SABRIC), 2023:np). The understanding of the nature of cyberfraud perpetrated can assist the South African banking industry to formulate measures to mitigate them. The findings reported in this study is based on the views of the bank experts consulted as well as those of the organisations. South African Banking Report (2019:np), mentioned that future works can consider the analysis of the level of effectiveness of the fraud control measures in the South African banking industry vis-à-vis the forms of cyberfraud identified.

Disclosure Statement

No potential conflict of interest was reported by the author(s).

References

Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2022), "Analytical hierarchy process decision model and Pareto analysis for mitigating cybercrime in the financial sector", *Journal of Financial Crime*, 29(3), 884-1008.

Ali, L., Ali, F., Surendran, P. and Thomas, B. (2017), "The effects of cyber threats on customer's behaviour in e-banking services*", International Journal of e-Education, e-Business, e-Management and e-Learning*, 7(1), 70-78.

Anti-Intimidation and Ethical Practices Forum (AEPF) (2020), "Unpacking fraud", pp. 1-9, [Online], available at: www.aepf.co.za/Unpacking_Fraud.pdf (accessed 16 November 2023).

Association of Certified Fraud Examiners (ACFE) (2012), "Managing fraud risk: first, second, or third line of defense responsibility?", United States of America, pp. 1-19, [Online], available at: www.acfe.com/uploadedfiles/acfe_website/content/european/course_materials/2012/11c_risch-cpp.pdf (accessed 2 February 2024).

Association of Certified Fraud Examiners (ACFE) (2019), "Anti-fraud technology benchmarking report", pp. K1-28, [Online], available at: www.acfe.com/uploadedFiles/ACFE_Website/Content/resources/Benchmarking_Technology_Report.pdf (accessed 2 May 2024).

Babbie, E. & Mouton, J. 2011. *The practice of social research*. Cape Town: Oxford University Press.

Babbie, E. (2021). *The practice of social research*. 15th edition. Australia: Cengage Learning.

Babbie, E. 2012. *The practice of social research.* Belmont: Wadsworth.

Bankscope (2018), "Bankscope Internet quick guide", [Online], available at: www.bankscope.bvdep.com (accessed 19 April 2024).

BusinessTech (2017), "Major SA banks taken to court over internet fraud", [Online], available at: https://businesstech.co.za/news/mobile/170629/major-sa-banks-taken-to-court-over-internet-fraud/ (accessed 1 August 2023).

Cassim, F. (2016), "Addressing the growing spectre of cybercrime in Africa: evaluating measures adopted by South Africa and other regional role players. School of law, university of South Africa", Based on a paper presented at the First International Conference of the South Asian Society of Criminology and Victimology (SASCV) at Jaipur, India from 15–17 January 2011, pp. 126-138.

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

Creswell, J.W. & Creswell, J.D. (2018). *Research design: qualitative, quantitative, and mixed methods approaches*. 5th edition. Thousand Oaks. SAGE Publications, Inc.

Creswell, J.W. & Poth, C.N. (2018). *Qualitative inquiry & research design-choosing among five approaches*. 4th edition. London: Sage Publications.

Creswell, J.W. (2020). *Research design.* 6th edition. Thousand Oaks (CA): SAGE.

Dagada, R. (2013), "Digital banking security, risk and credibility concerns in South Africa", The Second International Conference on Cyber Security, Cyber Peacefare and Digital Forensic (CyberSec2013), Kuala Lumpur, Malaysia, 4-6 March 2013.

Denscombe, M. 2012. *Research Proposals-A practical guide.* McGraw- Hill House: Open University Press.

DePoy, E. & Gitlin, L. N. 2016. *Introduction to Research: Understanding and Applying Multiple Strategies*. (5th Edition). USA: Elsevier.

Dlamini, S. and Mbambo, C. (2019), "Understanding policing of cybercrime in South Africa: the phenomena, challenges and effective responses", *Cogent Social Sciences*, 5(1), 1-13.

Dzomira, S. (2014), "Electronic fraud (cyber fraud) risk in the banking industry, Zimbabwe", Risk Governance and Control: *Financial Markets and Institutions*, 4(2),16-26.

Dzomira, S. (2015), "Cyber-banking fraud risk mitigation conceptual model*", Banks and Bank Systems,* 10(2), 7-14.

Ezejiofor, R.A., Nwakoby, N.P. and Okoye, J.F.N. (2016), "Impact of forensic accounting on combating fraud in Nigerian banking industry", *International Journal of Academic Research in Management and Business,* 1(1), 1-19.

Gbegi, D.O. and Adebisi, J.F. (2014), "Forensic accounting skills and techniques in fraud investigation in the Nigeria public industry", *Mediteranean Journal of Social Sciences*, 5(3), 243-252.

Isa, T. (2011), "Impacts and losses caused by the fraudulent and manipulated financial information on economic decisions", *Review of International Comparative Management*, 12(5), 929-939.

Joyner, E. (2019), "Enterprise-wide fraud management", Banking, Financial Services and Insurance, SAS Global Forum 2011, Cary, NC, SAS Institute.

KMPG (2019), "The Multi-Faceted threat of fraud: are banks up to the challenge?", Global Banking Fraud Survey, [Online], available at: www.kpmg.com (accessed 5 May 2024).

Kroll (2019), "Global fraud report: economist intelligence unit survey results", [Online], available at: www.kroll.com (accessed 1 April 2024).

Kumar, R. (2020). *Research methodology: A step-by-step guide for beginners*. 6th edition. Thousand Oaks, CA. SAGE Publications, Inc.

Kumar, R. 2011. *Research Methodology- a step-by-step guide for beginners*. (3rd Edition). London: SAGE Publications.

Kumar, R. 2014. *Research Methodology. A step-by-step guide for beginners.* (4th ed). London: SAGE.

Maxfield, M. & Babbie, E.R. 2018. *Research methods for criminal justice and criminology*. 8th edition. Boston, MA: Cengage Learning.

Maxfield, M. G. & Babbie, E. 2015. *Research Methods for Criminal Justice and Criminology*. Belmont: Wadsworth.

Maxfield, M. G. & Babbie, E. R. 2011. *Research Methods for Criminal Justice and Criminology*. Belmont, CA, Wadsworth Pub.

Modugu, K.P. and Anyaduba, J.O. (2013), "Forensic accounting and financial fraud in Nigeria: an empirical approach", International Journal of Business and Social Science, Vol. 4 No. 7, pp. 281-289.

Ndlovu., N. 2023. – © 2023 News Central Media. Banking app kidnappings: SABRIC on how not to become a victim. TechCentral asked SABRIC-CEO Nischal Mewalall about banking app kidnappings and how people can protect themselves. Available at: https://techcentral.co.za/banking-app-kidnappings-SABRIC-victim/234994/ (Accessed on 22 February 2023).

PwC (2016), "Banking in Africa matters – African banking survey", Global Fintech Report, pp. 1-100, [Online], available at: www.pwc.org (accessed October 2023).

PwC (2018), "Global economic crime survey: pulling fraud out of the shadows", pp. 1-30, [Online], available at: www.pwc.org (accessed 25 January 2024).

PwC's Global Economic Crime Survey (2020), "Global economic crime and fraud survey", (7th ed.), pp. 1-32, [Online], available at: www.corruptionwatch.org.za/wp-content/uploads/2020/06/global-economic-crime-survey-20201.pdf (accessed 17 January 2024).

Ramadani, S., Siahaan, A.P.U., Sutrisno, R.S., Amelia, W.R., Dalimunthe, H. and Munthe, R. (2018), "Impact of cybercrime on technological and financial developments", International Journal for Innovative Research in Multidisciplinary Field, Vol. 4 No. 10, pp. 341-344.

South African Banking Report (2019), [Online], available at: www.globenewswire.com/news-release/2019/02/20/1738270/0/en/South-Africa-Banking-Industry-Report-2018.html (accessed 1 June 2024).

South African Banking Risk Information Centre (SABRIC) (2022), "Digital banking crime statistics", [Online], available at: www.sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/ (accessed 5 June 2024).

South African Banking Risk Information Centre (SABRIC) (2023), "Annual crime statistics", [Online], available at: www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf (accessed 20 June 2024).

South African Reserve Bank (SARB) (2020), "Management of the South African money and banking system", [Online], available at: www.resbank.co.za/AboutUs/Functions/Pages/Management-of-the-South-African-money-and-banking-system.aspx (accessed 2 February 2024).

Sutherland, E. (2017), "Governance of cybersecurity – the case of South Africa", The African Journal of Information and Communication, Vol. 20, pp. 83-112.

Tiwari, S., Bhalla, A. and Rawat, R. (2016), "Cybercrime and security", International of *Advanced Research on Computer Science and Software Engineering*, 6(4), 46-52.

UK Finance (2018), "Staying ahead of cybercrime", pp. 1-16, [Online], available at: www.ukfinance.org.uk (accessed 20 January 2022).

Van Niekerk, B. (2017), "An analysis of cyber-incidents in South Africa", *The African Journal of Information and Communication*, 20, 113-132.

Wanemba, M.A. (2010), "Strategies applied by commercial banks in Kenya to combat fraud", A Management Research Project Submitted in Partial Fulfilment of the Requirements for The Award of the Degree of Master of Business Administration, Department of Business Administration, School of Business, University of Nairobi.