The Role of Bank Subject Matter Experts in the Investigation of Mobile Fraud in South African Banking Industry

Mokopane Charles Marakalala
College of Law, School of Criminal Justice, Law Department of Police Practice,
University of South Africa, Preller Street Muckleneuk Ridge, Pretoria, South Africa.
Corresponding authour: 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 https://www.ssrn.com/index.cfm/en/oida-intl-journal-sustainable-dev/

Abstract: Online banking is offered by the banking industry to give its clients quick and simple access to banking services. Nowadays, the majority of banking services are done online, which leads to concerning fraud every day. The frequency and severity of online banking frauds are rising worldwide, and they harm both banks and consumers. Investigating problems with online fraud detection in South Africa's banking industry was the aim of the study. In the South African context, the study found that the banking industry lacks specialists in online fraud. The results show that banks' detection systems may be inadequate due to a lack of experience with online fraud. From a South African standpoint, the study found that there is a high risk due to a lack of legal regulation. Banks are encouraged to acquire and develop online fraud expertise because the banking industry lacks these specialists. Since online banking technology is advancing more quickly than traditional transactions, rules and guidelines must be updated frequently to reflect the swift advancements in technology. Given the importance of international online banking, the study made recommendations for potential research topics that the banking industry could look into in order to create and improve online fraud detection models and stop online fraud.

Keywords: Bank, Consumer, Experts, Fraud, Investigation, Mobile, Models, Technology

Introduction

The use of mobile phones in banking has led to online banking fraud and digital identity, which is a problem affecting the South African banking industry. This type of online financial fraud manifests through hackers gaining access to a mobile device and using it to access accounts and confidential personal data. The option of online banking is used by millions of people worldwide to perform bank transactions quicker and easily. SABI also initiate the public on self-defense techniques and increase public awareness of fraud. Online Financial crimes prioritised by the SABI include fraud, money laundering, financing of terrorism, and cybercrime. Alerting the public awareness on various bank-related crimes and teaching people self-defense techniques are important tasks of the SABI. To fight financial crime, SABI encourages cooperation amongst regulatory agencies, payment processors, financial institutions, and other partners. Also, the SABI makes it easier to exchange information about new dangers and illegal activity. For example, the report shows statistics on financial crimes of all kinds: contact crimes, card fraud, and digital fraud. Also covered in the report are financial losses brought about by these crimes and the measures taken to prevent them.

As reported by reports of the SABI, online banking fraud and digital identity involve criminals targeting online mobile of bank customers who use banking applications (app) and Sim-swap.

- The requirement that mobile networks would gather biometric data does not adequately address online banking fraud and digital identity in SABI.
- The SABI released its first statistics on crime involving digital banking between 2018/2022. The report showed a marked increase in financial crime associated with nearly R3.3 billion in losses.

- The financial crime includes contact crimes, card fraud, and digital fraud, and they deter economic advancement in South Africa.
- Fraud involving digital banking has increased by 45%, associated with a 47% increase in financial losses and the highest increase recorded in cybercrime. online banking fraud and digital identity involving banking applications has become the most significant threat, accounting for 60% of all incidents linked to digital banking and soaring by an astonishing 89% each year.
- The research aims and objectives:
- The paper aims to explore the role of bank subject matters experts in the investigation of mobile fraud in SABI.
- To identify the role of bank subject matters experts in the investigation of mobile fraud in SABI.
- To determine the role of bank subject matters experts.
- To examine the models used to the investigate the mobile fraud.
- To demonstrate the best practice in the investigation of mobile fraud in SABI

Similar to this, the risk of mobile fraud in connection to ethics and good governance is described in the SABRIC annual report from 2028/2022 on SABRIC audits. One of the trickier frauds to investigate is mobile fraud. According to PricewaterhouseCoopers (2022:np) the act of perpetration was either carried out by singular persons or by coordinated efforts between several individuals or organisations. SABRIC (2021:np) argues that mobile fraud in SABRIC has a negative impact on banking sectors. To combat mobile fraud, the South African government primarily uses a framework for digital forensics and investigations that has been strengthened, statutory investigative bodies that have been established, and public anti-corruption campaigns that have been launched, appealing to the integrity of all people. The digital banking and financial technology have received most of the attention over the years, while biometric banking technology has received little to no attention. After considering the aforementioned problem statement, the researcher determined that the aim and objectives of the paper.

Literature Review

Setting the parameters for the study, gathering data through literature study (annual statistical reports-2018/2022) and visual materials, and developing the procedure for documenting material are all included assert that gathering data is the aspect of a research study that takes the longest. This task must be completed because without data, it would be impossible to increase one's knowledge base, provide an explanation for the 'unknown', or add new information to that which already exists. Unit of analysis: Six annual reports from 2018/2022 were analysed and they are:

- South African Banking Risk Information Centre (SABI);
- Association of Certified Fraud Examiners (ACFE);
- Global System for Mobile Communications Association (GSMA);
- Internet Service Providers' Association (ISPA);
- The International Criminal Police Organisation (INTERPOL);
- The Auditor-General of South Africa (AGSA).

A narrative literature review was used in this study as the primary mode of data collection, by conducting a review on the annual reports from 2018/2022. According to Khaldi (2017:25) data collection is the methodical collection of facts and figures. The following factors as Kumar (2021:164) explicitly states, must be taken into consideration when choosing a specific research method for gathering data:

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

- The socioeconomic-demographic characteristics of the research study.

Research Methodology and Methods used

This paper presents the research methodology and methods used. The research methodology talks to philosophical worldview, which is the research approach and design, then methods speak to the population, sampling method, data collection method, and data analysis techniques and procedure used. Furthermore, method to ensure trustworthiness will be discussed. It is also crucial that the researcher conduct research in accordance with accepted standards and the researcher adhered to ethical principles as discussed in this paper. A qualitative method was adopted to fulfil the purpose of the study. Non-probability sampling was used to select documents that were used to collect data, as this is a literature review study that mainly used secondary data as a source of information, including relevant national and international literature, about the role of bank subject matters experts in the investigation of mobile fraud in SABI. The researcher wanted to generate new knowledge with the purpose of empowering inhouse investigators who investigate mobile fraud cases in the South African Banking Industry (SABI). The purpose of this narrative literature review was to explore, analyse, describe the situation, and then suggest and recommend solutions to the problem identified. The information obtained from secondary data was analysed thematically. This study explore the role of bank subject matters experts in the investigation of mobile fraud in SABI. Following that, the findings indicated that the lack of online fraud expertise may lead to banks having weak detection systems. There is a lack of law regulation which poses high risks. Furthermore, this kind of study was necessary because it provides relevant information to investigators for:

- Investigative linkage of unsolved cases of mobile fraud in SABI;
- The development of investigative leads and suspect identity in unsolved cases by accumulating mobile fraud cases;
- To develop the forensics models for biometrics payments technology and digital payments techniques to combat mobile fraud.

Methods and materials

This section presents the methodology that is followed in this paper. The worldview that the researcher believe in is discussed (This implies papering phenomena drawing from non-empirical sources that include literature, artefacts, paintings or any other materials that talk to the question of the research). This is a desktop/literature paper, where the researcher adopted qualitative method (due to lack of participants for the online banking fraud and digital identity). Comprehending the theory and practical aspects of this application serve as the foundation for the desire to adopt a constructivist paradigm.

The approach adopted in this paper is qualitative

In the context of this paper, literature review from the following annual statistical reports: South African Banking Risk Information Centre (SABI), Association of Certified Fraud Examiners (ACFE), Global System for Mobile Communications Association (GSMA), Internet Service Providers' Association (ISPA), the International Criminal Police Organisation (INTERPOL) and the Auditor-General of South Africa (AGSA) annual statistical reports from 2018/2022), is perused and interpreted in relation to the research question which explored online banking fraud and digital identity.

The Philosophical Worldview

According to Creswell (2020:6), the philosophical worldview is crucial to research. When planning a study, researchers must consider the assumptions they bring to the study, the inquiry strategy that is connected to this worldview, and the particular research methods or procedures that put the approach into practice (Babbie & Mouton, 2021:66). There are various research worldviews, such as the pragmatic worldview, the advocacy/participatory worldview, the post-positivist worldview, and the social constructive worldview (Snyder, 2019:337; Kumar, 2020:45). The researcher conducted this investigation by means of the Social Constructive Worldview.

The worldviews

Postpositivist: This perspective places a strong emphasis on objectivity, the use of non-empirical data for literature studies, and the application of rigorous research methods to narrative literature reviews of mobile fraud. Leavy (2022:67) indicates that postpositivist research on banking subject matter reflects the need to pinpoint and investigate the factors that affect results (Creswell, 2020:13).

Constructivism: Creswell (2020:16) indicated that qualitative research techniques are used to investigate secondary data analysis viewpoints, as this worldview is centred on comprehending the significance of experiences and the social construction of knowledge.

Pragmatism: This problem- centred worldview employs a range of techniques to solve real-world issues and concentrates on the beneficial effects of decisions.

Distinctive Methods and Subtypes

It is typical to think of the narrative review as an umbrella phrase that encompasses a number of different review subcategories (Greenhalgh, *et al.,* 2018:55) These narrative subgenres share the goal of increasing knowledge of a subject while also explaining the rationale behind a researcher's choice to investigate and analyse the subject in a certain manner.

Narrative literature reviews come in a number of forms, employing diverse methods, each providing a different perspective on how to analyse and interpret the literature and address the research topic. The forthcoming SABRIC special articles on reviews will also discuss the popular narrative review kinds addressed in this thesis which are theory integration, critical, meta-ethnographic, and state-of-the-art reviews.

A *state-of-the-art review* strives to compile a study on a given subject along a timeline of keyshifts in knowledge orresearch approaches. State-of-the-art reviews concentrate on these turning points in the history of our changing understanding of phenomenon, providing a synopsis of the present state of knowledge, how that understanding was created, and a glimpse into potential future paths (Ferrari, 2015:234).

A *meta-ethnographic review* choosing and analysing qualitative information on a specific issue is part of a meta-ethnographic study. This sort of knowledge synthesis makes use of just qualitative data in an attempt to come to new understandings or conclusions about a topic (Greenhalgh *et al.,* 2018:69). It integrates qualitative research findings with analyses from past publications to produce new knowledge that encompasses these occasionally modest, individual studies.

A *meta-narrative review* aims to understand and analyse inconsistencies and contradictions in the literature. The meta-narrative review, which maps out the various interpretations of a particular topic, carries conducts a focused investigation to define and contrast stories, and then, as part of the analysis, seeks to understand how these stories are interpreted in different fields or historical contexts (Greenhalgh *et al.,* 2018:56).

A *critical review* using an interpretive lens, the review is a synthesis of literature: the review is shaped by a theory, a critical viewpoint, or viewpoints from other fields. areas for literary analysis guidance. According to Greenhalgh *et al.,* (2018:58), critical reviews use an interpretive method that combines the reviewer's theoretical framework with well-known theories and models in order to make things easier. the integration and analysis of data from several research investigations.

Reviewers first establish and describe their interpretive theoretical viewpoint, which is shaped by their own skills and experiences. Key themes pertaining to a research topic are then identified and collected through a partial search.

An *integrative review* generally takes one of two distinct orientations. Publications of evidence-based studies with different methodologies are analysed and synthesised by empirical integrative reviews. Conversely, theoretical integrative reviews analyse the available theories that address a phenomenon, offer a critique of those theories, and suggest a step forward in their development (Greenhalgh, *et al.,* 2018:62). Both kinds of integrative reviews adhere to a multistage process that includes identifying the problem, looking for it, evaluating it, analysing it, and presenting it.

As noted by Creswell (2020:16), the Social Constructivist Worldview is a viewpoint and is commonly regarded as a method for qualitative research. Additionally, Creswell explains that social constructivism is predicated on the idea that people try to comprehend the world in which they live and work. Exploring biometric-based solutions to combat mobile fraud at SABRIC and comprehending the theory and practical aspects of this application serve as the foundation for the desire to adopt a constructivist paradigm. In order to further investigate biometric-based solutions for preventing mobile fraud in the area under investigation, this will be explained in detail and will benefit SABRIC. Qualitative research follows the anti-positivist worldview. The proponents of anti-positivism subscribe to the theoretical posture that postulates epistemology as the basis for research. This implies studying phenomena drawing from the lived experiences of persons involved with phenomena being studied, or from direct empirical sources that include literature, artefacts, paintings or any other materials that address the question of the research.

Target Population and Sampling

Study Population

The researcher targeted secondary data relevant to the study as sources of information. The data used were obtained from the following annual statistical reports: SABRIC, ACFE, GSMA, ISPA, INTERPOL) and AGSA annual statistical reports from 2018/2022) that were used to choose the sample referred to as the population and generalise the study's findings (David & Thomas, 2018:33; Creswell, 2020:29). The term universe refers to all subjects that have the characteristics that the researcher is interested in, for instance all people who live in the world and have obtained a post-graduate degree.

Snyder, (2019:66).posit that the word 'population' was used for narrative literature reviews and on statistic annual reports 2018/2022 that could be included in a study. It could also be objects, subjects, phenomena, the SABRIC annual report, events and activities that the researcher wishes to research to establish new knowledge. The annual statistical reports-2018/2022 made up the population of this study. In the opinion of Saunders, Lewis and Thornhill, 2019:86); Bachman and Schutt (2015:106) it is imperative for a researcher to establish the 'parent population' before defining any number of units of analysis. When a sample needs to be chosen, this would represent the entire population. The above-mentioned writers contend that in order to determine the population for a research project, three important questions need to be addressed (Saunders *et al.,* 2017:87; Bachman *et al.,* 2015:112). The research question, which is outlined below, must provide the basis for these inquiries. They might affect the final result of the research if they are not appropriately accessed. The research questions, which are outlined below, must provide the basis for these inquiries. They might affect the final results if they are not appropriately accessed. The questions must:

- Clearly establish whether any specific sub-sets of the population need to be excluded because of the prevalence of certain scenarios or experiences
- It must also be ascertained whether any additional sub-population needs to be included. The literature review discusses, and analyses published information from the annual statistical reports from 2018/2022 that are now available, and which have been determined to be the parent population for this qualitative research study. Official authorisation from SABRIC was obtained to do data analysis.

Sampling Procedures

In this study, an inquiry narrative literature review, selected from a population is referred to as a sample. Finding accurate information about the sample is the aim. It is up to the researcher g to choose how to monitor the annual statistical reports from 2018/2022. Sampling, which is utilised for data generation by any means, relates to the concepts and practices used to locate, select, and obtain access to pertinent units. The fundamental idea behind sampling is that reliable results can be obtained without having to obtain information from every member of the 'population' being surveyed (Denscombe, 2012:23). Non-probability sampling is a strategy in which the researcher chooses samples based on the researcher's subjective judgment rather than random selection. Probability sampling is used when the probability of the chosen population elements has not yet been defined. According to Denscombe (2012:23) and Bachman *et al.,* (2015:108) it is a less rigorous approach. Non-probability sampling was the method of choice for this study and was used extensively. According to Maree (2017:80) and Welman *et al.,* (2011:56) all authors mentioned before? non-probability sampling should be used instead of random selection when conducting research because it eliminates the need for random selection when selecting a research sample. Similarly, Hennink, Hutter and Bailey (2020:98) argue that non-probability sampling is aligned with qualitative research.

The foundational data for this research came from the narrative literature reviews (annual statistical reports-2018/2022) that were specifically related to mobile fraud. A five-year basis data set was purposefully chosen by the researcher using the following justification:

- To get an understanding of the past and current MO types perpetrated into mobile fraud at SABRIC and to determine similarities, if any.
- To align with the aim of this research and the research questions as defined, identified as crucial from an accuracy and completeness perspective for qualitative research.

Results and Discussion

As highlighted the aim of this paper is to explore the prevalence, causes, and consequences of biometric-based solution in combatting online banking fraud and digital identity at SABI. Consistent with this research aim, the developed themes and consequent findings of the paper were generated in response to the following objectives:

To identify the role of bank subject matters experts in the investigation of mobile fraud in SABI

Subject matter experts check details and facts to ensure a project-created deliverable meets technical requirements and follows best practices, company policy and current law. More specific responsibilities of SMEs include:

- Working with company leadership to define project objectives, processes, policies, procedures and rules;
- Explaining policy implementation to fellow team members;
- Getting management approval or approving alterations in rules, procedures and policies;
- Informing consumers regarding project goals and expected deliverables;
- Resolving project-related problems within their area of expertise;
- Fact-checking other professionals on the project to ensure data and information accuracy;
- Providing feedback to project team throughout creation, testing and rollout of deliverables;
- Working with company leadership to create testing scenarios and validate test results;
- Performing user-acceptance testing at the end of the project;
- Validating deliverables produced by a project or company;
- Creating project-related documentation and training manuals;
- Teaching or training project employees and consumers;
- Communicating with company stakeholders regarding project progress;
- Serving as an expert witness in legal cases.

Skills for SMEs

Successful subject matter experts possess several key skills, including:

- Deep understanding of a subject

SMEs possess a masterful understanding of their area of expertise. Most SMEs achieve this through a combination of formal education, self-guided instruction and years of work experience. Employer’s value these individuals for the specialization they can provide in more niche subject areas.

- Commitment to relevancy

It's important that SMEs remain up to date on any changes in industry practices or protocols to maintain their reputation and continue achieving workplace success. SMEs stay ahead of industry trends and advances by reading professional journals, furthering their education and networking with other professionals. Networking is an especially helpful way to remain relevant in a field through interpersonal communication via phone, email, social media or in-person meetings.

- Communication skills

A vital task for any subject matter expert is the sharing of knowledge with team members. Successful SMEs can explain highly technical information in a way that is understandable and usable. SMEs also ask questions to ensure they understand the needs of their clients and team members. SMEs also deliver information in a timely, useful fashion, and training and teaching sessions should help learners understand key points in a short time.

- Working on a team

Teamwork is a valuable skill in most work environments, and the same goes for those pursuing a career as a subject matter expert. SMEs often work on time and budget-sensitive projects with professionals from varied backgrounds and experience levels. Successful subject matter experts can benefit from working cooperatively with diverse groups of people, boosting their reputation and increasing connections simultaneously.

- Ability to problem-solve

A subject matter expert's attention to detail and extensive knowledge base allows them to identify and solve problems as they arise in a project. As the foremost authority on their specific subject, it's important that they can handle unforeseen obstacles and using their extensive knowledge to overcome them. When teaching and training, SMEs may need to develop novel methods for communicating complex information to team members in other disciplines.

To examine the models used to the investigate the mobile fraud

The fraud triangle is a model that explains the motivations behind fraudulent behavior through three key elements: pressure, opportunity, and rationalization. Developed in the 1950s by criminologist Donald Cressey, the model suggests that individuals are likely to commit fraud when they experience financial pressure, have the opportunity to execute fraudulent acts, and can justify their actions to themselves. Common pressures that may lead to fraud include financial emergencies due to personal circumstances like medical issues or addictions. Opportunities for fraud often arise from weak organizational controls, allowing individuals access to financial resources. Rationalization enables fraudsters to convince themselves that their actions are justified, often viewing it as a temporary borrowing or a response to perceived wrongs by employers.

While the fraud triangle has been a widely used tool in fraud prevention and detection, some scholars question its comprehensiveness, suggesting it may not adequately capture all motivations behind fraud. Critics point to cases like that of a well-paid executive committing fraud without evident financial pressure, arguing that some individuals may engage in dishonest behavior simply because they can. Overall, understanding the fraud triangle can aid organizations in identifying potential fraud risks and reinforcing ethical standards to mitigate these risks.

The Triangle: Pressure, Opportunity, and Rationalization

According to the fraud triangle model, people must have three specific points to commit fraud. The first part of the fraud triangle is pressure. The *pressure* is a financial need or perceived financial need that triggers a person to look for money from outside their normal sources. When the person's financial need cannot be alleviated by legitimate sources, the person may consider fraud. Some common sources of pressure include divorce, buying or renovating a house, personal medical problems, family medical problems, gambling, and alcohol or drug addiction.

The *opportunity* point of the fraud triangle indicates that individuals who commit fraud must have the ability to commit the fraud. In most organizations, only certain people are positioned to commit fraud because they have access to the company's financial accounts and information. In other instances, businesses and organizations have weak controls in place, giving more people an opportunity to commit fraud.

The third point of the triangle is *rationalization,* meaning fraudsters can justify or rationalize their actions in many ways. Some people rationalize their actions because they say they are just borrowing the money and will pay it back. Others rationalize the fraud in other ways, including by telling themselves they are righting a wrong that was done to them by their company or organization.

To demonstrate the best practice in the investigation of mobile fraud in SABI

Mobile fraud remains a major concern at SABRIC and in any sector that involves the management of finances. Although ripe with positive innovation, new SABI (Nedbank, FNB, ABSA, STD and Capitec) channels and solutions also mean new avenues for fraudulent activities to take place and new vulnerabilities that can be exposed (Button *et al.,* 2017:18). Players across the ecosystem need to work together and continually improve security measures to keep bad actors at bay and protect the funds and data of the end users they serve (INTERPOL, 2020:np). Below is the presentation of best practices that may be applied in the prevention of mobile fraud:

Continuous monitoring and adaptive strategies: Proactive actions and continuous observation are necessary for the continuous process of fraud prevention. Companies should invest in sophisticated fraud prevention tools, regularly

train staff on fraud detection techniques, conduct thorough audits to identify risks and vulnerabilities, and review and update their fraud prevention strategies to stay ahead of evolving threats (AGSA, 2019:np).

Education for end users: When providing goods and/or services directly to customers, it is critical to make sure they are equipped with the most recent information necessary to use products securely. By providing end users with fraud education, they may protect their financial resources by making wise judgments and taking the necessary precautions (Brytting *et al.,* 2019:101). Customers are less likely to become victims of fraud unintentionally if they are aware of prevalence scams or risks related to certain fintech goods. From the bottom up, user-initiated alerting systems can be helpful in highlighting any unauthorised or questionable activity occurring on a financial platform (AGSA, 2022:np). Provide an easily accessible route, like a dedicated fraud reporting hotline or email address, for customers to report fraudulent activities. Encourage users to report any suspicious or unlawful transactions as soon as possible (Button *et al.,* 2017:22).

The mobile fraud detection challenges faced by subject matter expects and underneath are discussions based on the figure:

Create a potential mobile fraud risk profile: This pertains to a top-down approach to risk assessment, which outlines the business units and types of mobile fraud that could happen in the locations where mobile fraud is most likely to happen (ACFE, 2022:np).

Next, as part of the overall risk assessment, it is necessary to categorize the risks based on the organisation's entire risk exposure and create risk profiles for mobile fraud that involve all stakeholders and decision-makers.

Address the possible indicators of mobile fraud: While sampling might be helpful for identifying issues that are generally consistent across datasets, this is not always the case when mobile fraud is involved. Instead, organisations should evaluate all of their data. Mobile fraud transactions are by their very prevalence premeditated (ACFE, 2022:np). It is said that transactions may not be reported even when they fit under the parameters of some regular tests.

Implement continuous auditing and monitoring: Continuous auditing and monitoring can be used to assess and validate the efficacy of an organisation's controls over transaction authorisations. Continuous analysis could involve writing scripts to identify anomalies as they appear over time (PwC, 2022:np). The total effectiveness, consistency, and quality of SABRIC in the mobile fraud process can all be significantly enhanced by this procedure.

Increase organisational awareness of the monitoring activity: One crucial component of combatting mobile fraud within the firm is the programme internal communication, which serves as a valuable tool for doing so (PwC, 2022:np). If employees are aware of the preventative measures that have been implemented, they would not engage in mobile fraud, which can be a very successful preventive strategy (Button *et al.,* 2017:93).

Encourage mobile fraud suspicious activity reporting: Finding clients implicated in financial crime or mobile fraud is the goal of the investigation that follows Suspicious Activity Reporting (SAR) (Omar & Bakar, 2012:15). A specific behaviour could be included in SAR if it gives rise to suspicions that the account holder is trying to hide anything or carry out an illegal transaction. As a result, businesses must put policies in place to report financial irregularities connected to mobile fraud (Button *et al.,* 2017:63).

Deploy intelligent case management: According to the AGSA (2022:np), utilise an advanced, analytics-driven, intelligent case management solution that can automatically assist in the following ways:

- Set case priorities, suggest investigative measures, and expedite simple cases;
- Add information to alerts regarding related accounts, beneficiaries, or customers;
- locate and retrieve data with intelligence from a third-party data source or from an internal database;
- Display information in comprehensible graphic aids;
- SAR should automatically fill out and be ready for electronic filing, if required.

The SABRIC can streamline their mobile fraud investigations by deploying an intelligent case management solution to aid their fight against cybercrimes (KPMG, 2013:19).

Learn, adapt and repeat: Reviewing, reassessing, and restructuring one's mobile fraud profile is necessary in order to move investigative lenses in line with the most prevalent mobile fraud schemes as well as those that are mainly related to the risks that are particular to organisation (INTERPOL, 2020:np). This can be accomplished by monitoring controls

that application control settings cannot control and by utilising data analytics to identify ineffective or non-functioning control areas (Omar & Bakar, 2012:66). Lastly, patterns and mobile fraud indicators shown by mobile fraud detection tests and continuous monitoring and auditing processes need to be investigated.

Mobile fraud reporting policy and procedure: Managers must be aware of what to do in the event of a scam or any alarming sign of mobile fraud so that they can act quickly (Patidar & Sharma, 2021: 2233).

According to the National Treasury (2020:34), the goal of the mobile fraud reporting policy and procedure is to ensure that action may be performed quickly and effectively:

- To prevent losses of funds or other assets and to maximise recovery of losses where mobile fraud has occurred;
- To minimise the occurrence of mobile fraud by taking rapid action at the first signs of a problem;
- To identify the mobile fraudsters and maximise the success of any disciplinary or legal action taken;
- To minimise any adverse publicity for the organisation suffered as a result of mobile fraud;
- To identify any lessons learnt and use these to prevent mobile fraud in the future; and
- To reduce adverse impacts on the business of the organisation.

The statement by the ACFE (2020:np) report acknowledges the existence of a mobile fraud reporting policy and procedure which may, in itself, help to act as a deterrent, as it shows that an organisation or a company is prepared to defend itself against the risk of mobile fraud:

- To reduce the possibility of identity theft and allow businesses to confirm the identity of their clients. Through the collection of pertinent data and comprehensive identity verification procedures, businesses may create a solid base for preventing fraud;
- **Encryption, Multi-Factor Authentication (MFA),** and frequent security audits are examples of data security techniques that can help protect sensitive data from unauthorised access;
- **The application of AI and Machine Learning (ML):** This has the potential to improve fraud detection performance to a great extent. These technologies are capable of real-time analysis of enormous volumes of data in order to spot trends and abnormalities that could point to or highlight fraudulent activity;
- The statement by Kumar (2024:71) indicted that this is incomplete to replicate identifier, biometric authentication which uses fingerprint or facial recognition which can increase user account security and lower the danger of unauthorised access;
- Transaction monitoring: Real-time transaction monitoring systems that examine consumer behaviour and transaction trends are helpful to identify hazards or possible fraud before it spreads (Button *et al.,* 2017:109). Creating guidelines and standards to identify suspicious activity, such as transactions that are abnormally big, occur frequently in a short period of time, or originate from high-risk areas, is an essential part of a solid security foundation;
- **Two-Factor Authentication (2FA):** Requesting an extra authentication factor from clients, such as a special number sent to their mobile device, can aid in confirming their identity while logging in or conducting high-risk transactions;
- **Device recognition:** It can be used to recognise and verify client devices that are used to access accounts or start transactions. This assists in identifying and thwarting attempts at fraud from unidentified or hacked devices. Using behavioural analytics, one can analyse and find anomalies in consumer contact patterns. By establishing baseline behaviours for each customer, unusual activities, such as sudden changes in transaction types or deviations from established patterns, can be flagged for investigation. Pattern recognition: these algorithms can help identify similarities and correlations among fraudulent activities across different customer accounts. Identifying patterns can detect fraud rings or organised fraud attempts.

Research Finding and Recommendation

In this paper, the researcher described stages involved in collecting and analysing the data consulted and studied for this study. Additionally, this paper presented the research findings emanating from the six annual reports from

2018/2022 that were sampled to answer the questions posed by the researcher during data collection sessions. In that regard, the criticality of the present paper is underpinned by the interpretation of the research findings which it serves as the most pivotal reference point for the much-needed practical evidence of the study in relation to both the research problem and aim of the study. By implication, the evidence of the study provides extensive details concerning the sampled narrative literature review (annual statistical reports-2018/2022), profound perspectives, knowledge, perceptions, experiences, and thoughts regarding the investigated phenomenon i.e., the role of bank subject matters experts in the investigation of mobile fraud in SABI annual statistical reports, ACFE annual statistical reports, GSMA, ISPA and the AGSA reports from 2018/2022 (Vithal & Jansen, 2019:65; Creswell & Poth, 2018:47).

This paper reported on the findings of the study and mapped out the findings in light of the narrative literature review that was analyses in the process of resolving the identified problem of mobile fraud at SABRIC. This research aimed to contribute the role of bank subject matters experts in the investigation of mobile fraud in SABI. Following the narrative literature review (annual statistical reports-2018/2022), the paper continued with a concerted presentation of discussions emanating from the narrative literature review (annual statistical reports-2018/2022), viewpoints, knowledge, thoughts, and understanding regarding the investigated phenomenon of the role of bank subject matters experts in the investigation of mobile fraud in SABI under SABRIC jurisdiction.

This paper presented the recommendations and conclusions based on the cited published literature as well as from: SABRIC. ACFE, GSMA, ISPA, INTERPOL and the AGSA annual statistical reports from 2018/2022. Furthermore, limitations of the study are sketched and the need for further research is stated.

It is recommended that SABRIC must adopt new innovative and secured mechanisms of financial dealings to enhance innovation, security and flexibility to combat mobile fraud. Also, the institution should provide forensic investigators and banking subject matter specialists with regular opportunities for more regular and more rigorous in-service training to acquire knowledge and skills. Such training should entail the following, as posited by the ACFE (2022:np):

- SABI fraud tactics become increasingly sophisticated, as it is continuously seeking innovative solutions to verify users securely, protect sensitive information, safeguard their customers, and prevent fraud. Biometric verification is emerging as one of the most powerful tools in this struggle to keep abreast. Gaining rapid traction, this biometric technology provides a secure and efficient way to verify and authenticate users and protect systems.
- SABRIC is adopting biometric solutions to strengthen security, protect sensitive data, and enhance user experiences, making it a cornerstone of modern fraud prevention strategies. This thesis explored the growing impact of biometric verification in fortifying security and combatting mobile fraud.
- De-escalation strategies involving the use of biometric technology and precautionary measures when responding to active crime scams should be actively sought and implemented.
- Inculcation of self-control and self-discipline for dignified behaviour that does not bring discredit to themselves and their organisation on, and off duty, and to also be discreet in their social behaviour and public appearances;
- Initiate processes for amending the constitution to include implementation of harsher sentences, such as life imprisonment for mobile fraud to deter reoccurrences;
- Review internal policies and procedures to ensure the implementation of proper safety measures and procedures that will increase the safety of the forensic investigators and banking subject matter specialists;
- Engage members of the community for restoration of trust and confidence among all the relevant stakeholders by hosting public awareness campaigns and educational road shows through social media, radio and television to eliminate any hostility or any enmity between communities, the forensic investigators and banking subject matter specialists.

Originality of contribution, implications, and avenues for further research

The structure illustrated in figure 5.1 provides guidelines for a Mokopane Fraud Model-24. Law Enforcement Agencies and SABI can be flexible in developing a model suitable for their circumstances.

Mokopane Fraud Model-24 recommend that SABI can work together with the following law enforcement agencies: - SAPS, HAWKS, Special Investigation Unit, Border Management Authority, Traffic Officers and service providers: -

MTN, Vodacom, C-Cell and Telkom to combat online banking fraud and digital identity and app kidnapping relating to the transaction of money (SABI annual statistical reports-2018/2022).

This paper identifies areas that need more research and contributes to the effectiveness and efficiency of the country's online banking fraud and digital identity investigation. In addition to academics and academic institutions, the following implications of the paper's findings would be beneficial to the entire corporate sector, the Criminal Justice System (CJS) and the global community.

Conclusion

This paper presented recommendations and conclusions. In this study, it is concluded that digital evidence is the most reliable form of evidence in mobile fraud when compared with other types of biometric-based solutions in combatting mobile fraud that are subject to manipulation. Both primary or secondary evidence and available literature reveal that several factors including lack of experience and qualifications in crime scene management contribute to some prevalence to evidence contamination (annual statistical reports-2018/2022). The findings of this study also reveal that there are set procedures that should be followed when managing a mobile fraud and collecting digital evidence and a failure to adhere to these procedures can lead to evidence contamination. Overall, the insights that emerged from the secondary data were confirmed by the available literature, which meant that the set objectives of this study at the beginning were achieved.

Based on the findings of this study and its attendant recommendations, the following conclusions were drawn:

- It is essential to involve and engage the community to build trust between the banks and the public in order to combat mobile fraud.
- It is crucial to work towards improving training, adequate resources, and better management style and to keep up with technology as SABRIC subject matters experts are in the Fourth Industrial Revolution.
- It is crucial to review the existing policies and guidelines to ensure that they are under nationally prescribed best practices, which will help to improve biometric-based solutions in combatting mobile fraud.

Furthermore, SABRIC ensures that only authenticated individuals are granted access, which markedly lowers risks such as identity theft and fraudulent account creation. It is advised that by utilising infrared light, the technology delineates the vein pattern and establishes a template for comparison. This technique is extremely secure due to the fact that vein patterns are hard to duplicate and maintain consistency over a person's lifespan. Some financial institutions and healthcare organisations implement vein recognition, adding an extra layer of security for identity confirmation. Furthermore, they ought to evaluate the effectiveness of their existing controls regularly in relation to newly arising fraud threats. Each of these biometric identity verification techniques is crucial in bolstering security, minimising fraud, and enhancing user experience. As technology progresses, these techniques are becoming more prevalent in both personal and professional settings, assisting organisations in better safeguarding sensitive data and facilitating smooth authentication processes.

List of References

1. ACFE. 2021. Fraud 101: What is Fraud? Available at: https://www.acfe.com/fraud-resources/fraud-101-what-is-fraud (Accessed on: 16 January 2023).
2. ACFE. 2022. Occupational fraud. A report to the nations. Available at: https://www.acfe.com/-/media/files/acfe/pdfs/rttn/2022/2022-report-to-the-nations.pdf (Accessed on: 16 January 2023).
3. Afonin, O. & Katalov, V. 2016. *Mobile fraud – advanced investigative strategies*. Birmingham: Packt Publishing
4. AGSA. 2021. Annual report for fraud. Available at: https://www.agsa.co.za/Reporting/AnnualReport.aspx (Accessed on 11 March 2023).
5. AGSA. 2022. Annual report for fraud. Available at: https://www.agsa.co.za/Reporting/AnnualReport.aspx (Accessed on 11 March 2023).
6. Albrecht, C., Holland, D., Malagueno, R., Dolan, S., & Tzafrir, S. 2015. "The role of power in financial statement fraud schemes". *Journal of Business Ethics,* 131(4), pp. 803–813.
7. Ambe, K.N. 2024. Analysis of the risk associated with bank crimes in Africa. *SSRN 4708322*.
8. Aurini, J. D., Heath, M. & Howells, S. 2016. *The how to of qualitative research*. London: Sage.
9. Babbie, E. & Mouton, J. 2021. *The practice of social research*. Cape Town: Oxford University Press.

10. Babbie, E. 2021. *The practice of social research*(15th edition). Australia: Cengage Learning.
11. Barker, R. 2018. Knowledge management to prevent fraudulent e-banding transactions. *Communitas*, 23(1), 71–86.
12. Bertram, C. & Christiansen, I. 2014. *Understanding Research: An Introduction to Reading Research.* Van Schaik, Pretoria.
13. Bezuidenhout, R. 2021. *Research matters* (2nndedition). Cape Town: Juta & Company Limited.
14. Bougie, R. & Sekaran, U., 2016. *Research methods for business: A skill building*(7th edition). India: Wiley Publishers.
15. Brandl, S.G., 2017. *Criminal investigation*. Sage Publications.
16. Brown, K., & Smith, J., 2022. The Role of Quantitative Finance in Financial Market Analysis and Decision-Making. *Financial Analysts Journal,* 78, 44-60.
17. Brungs, A., Winchester, D., Stephens, G. & Smith, S., 2018. The power of hermeneutic phenomenology in restoring the centrality of experiences in work-integrated learning. *International Journal of Work-Integrated Learning*, 19(3), pp. 261-71.
18. Bryman, A. 2012. *Social Research Methods.* Oxford: Oxford University Press.
19. Bryman, A. 2021. *Social research methods*(6th edition). Cape Town: Oxford University Press.
20. Brytting, T., Minogue, R. & Morino, V. 2019. *The Anatomy of Fraud and Corruption: Organisational Causes and Remedies.* Britain: Gower Publishing Ltd.
21. Buckles, T. 2017. *Mobile fraud Scene Investigation: Criminalistics and the Law*. New York: Thomson Delmar Learning.
22. Burrell, D.N. 2023. *Transformational interventions for business, technology, and healthcare*. IGI Global.
23. Button, M. and Cross, C., 2017. *Cyber frauds, scams and their victims*. Routledge.
24. Casey, E. 2021. *Digital evidence and computer crime* (3rd ed). Massachusetts: Academic Publishing.
25. Caulfield, T. & Steckler, S. 2014. "*The five faces of Mobile fraud, abuse, and noncompliance*", Contract Management, Vol. December, pp. 38–45.
26. Cressey, D. R. 1953. *Other people's money: a study in the social psychology of embezzlement*. Glencoe, IL: The Free Press.
27. Creswell, J. W. & Poth, C.N. 2018. *Qualitative inquiry & research design-choosing among five approaches*(4th edition). London: Sage Publications.
28. Creswell, J.W. 2020. *Research design* (6th edition). Thousand Oaks (CA): SAGE.
29. David, R. & Thomas, I.H. 2018. *Designing and planning your research project: Core skills for social and health research*. Chicago: Sage Publications.
30. De Vos, A., Strydom, H., Fouche, C. & Delport, C. 2011. *Research at Grass Roots: For Social Sciences and Human Services Professions*. South Africa: Van Schaik Publishers, Pretoria.
31. Denscombe, M. 2012. *Research Proposals-A practical guide*. McGraw- Hill House: Open University Press.
32. DePoy, E. & Gitlin, L.N. 2016. *Introduction to Research: Understanding and Applying Multiple Strategies* (5th Edition). USA: Elsevier
33. Ferguson, G. 2017. *Global corruption: law, theory and practice* (3rd edition). Victoria: University of Victoria.
34. Ferrari, R., 2015. Writing narrative style literature reviews. *Medical writing*, *24*(4), pp.230-235.
35. Flick, U. 2020. *Introducing Research methodology: A beginner guide to doing a research project*. London: SAGE.
36. Girard, J. E. 2021. *Criminalistics: Forensic Science and Mobile fraud*. Burlington: Jones and Bartlett.
37. Global System for Mobile Communications Association [GSMA]. 2022. Mobile money fraud typologies and mitigation strategies. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2022/03/GSMA-Fraud-Typologies-.pdf (Accessed on 11 March 2023).
38. Gray, D. E. 2019. *Doing Research in the Real World* (5th edition). London: SAGE Publication.
39. Hennink, M., Hutter, I. & Bailey, A. 2020. *Qualitative research methods* (2nd edition). Sage Publications.
40. INTERPOL. 2020. Interpol Warns of Financial Fraud Linked to COVID-19. Available at: http://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-warns-of-financial-fraudlinked-to-COVID-19 (Accessed on 10 July 2023).

41. INTERPOL. 2021. The two banks with the biggest increase in complaints in 2021. https://www.moonstone.co.za/the-two-banks-with-the-biggest-increase-in-complaints-in-2021/ (Accessed on 10 July 2023).
42. ISPA. 2020. Available at: Internet-Service-Providers-Association-ISPA-Submission-MDPMI-Provisional-Report-2022.pdf (Accessed on 07 April 2023).
43. ISPA. 2021. Available at: Internet-Service-Providers-Association-ISPA-Submission-MDPMI-Provisional-Report-20230407.pdf (Accessed on 07 April 2023).
44. ISPA. 2022. Available at: Internet-Service-Providers-Association-ISPA-Submission-MDPMI-Provisional-Report-2022pdf (Accessed on 07 April 2023).
45. James, S.H. & Nordby, J. 2018. *Forensic science. An introduction to Scientific and Investigative Techniques* (3rd edition). Boca Raton: CRC Press.
46. Khaldi, K. 2017. Quantitative, qualitative or mixed research: Which research paradigm to use. *Journal of Educational and Social Research*, 7(2), pp. 15-24.
47. KPMG. 2013. KPMG Malaysia Fraud, Bribery and Corruption Survey and Others. Available at: https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/fraud-survey-report.pdf (Accessed on 09 May 2022).
48. Kruse, C., 2015. *The social life of forensic evidence*. Univ of California Press.
49. Kumar, R. 2020. *Research methodology: A step-by-step guide for beginners* (6th ed.). USA: SAGE Publications Inc.
50. Kumar, R. 2021. *Research Methodology- a step-by-step guide for beginners* (7th ed.). London: SAGE Publications.
51. Leavy, P. 2022. *Research design: Quantitative, qualitative, mixed methods, arts based, and community-based participatory research approaches*. New York: The Guilford Press.
52. Leedy, P. D. & Ormrod, J. E. 2016. *Practical Research: Planning and Design* (11th ed.). Upper Saddle River: Pearson Education. Inc.
53. Machi, L.A. & McEvoy, B.T. 2016. *The literature review: Six steps to success* (3rd edition). Los Angeles: Corwin Press.
54. Mason, J. 2018. *Qualitative researching* (3rd edition). London: Sage.
55. Maxfield, M. & Babbie, E. R. 2018. *Research methods for criminal justice and criminology*(8th edition). Boston, MA: Cengage Learning.
56. Maxfield, M.G., Babbie, E.R. & Schuck, A.M. 2011. *Research methods for criminal justice and criminology*. Belmont, CA: Wadsworth Cengage Learning.
57. Murimbika, S. 2024. Surveying the reputation-regulation interface in the SABI industry: Perspectives of private banking customers. *South African Journal of Business Management*, 55(1), p.3901.
58. National Treasury. 2020. *Fraud Prevention Plan*. Pretoria: Government Printer.
59. Nayab, N. 2020. How to determine validity in qualitative research. Project management methods and ideologies. USA: Bright Hub PM.
60. Ombudsman for Banking Services. 2022. New wave of fraud targeting banking customers. Available at: https://www.obssa.co.za/press_releases/new-wave-of-fraud-targeting-bank-customers/ (Accessed on 29 May 2023).
61. Open Data Charter. 2018. *Using data to combat corruption*. https://open-datacharter.gitbook.io/open-up-guide-using-open-data-to-combatcorruption/background-charter-open-up-guides (Accessed on 14 April 2022).
62. Panigrahi, S., Kundu, A., Sural, S. & Majumdar, A. K. 2007. Use of dempster-shafer theory and Bayesian inferencing for fraud detection in mobile communication networks, in: *Information Security and Privacy*. Springer.
63. PASA. 2016. Card fraud 2016: protect your card and information at all times. Available at: https://www.SABRIC.co.za/media/1038/2016-card-fraudbooklet.pdf (Accessed 24 April 2022).
64. Patel, F. 2023. The Citizen. SA grappling with a surge in banking app fraud, SABRIC reveals. Available at: https://www.citizen.co.za/news/sa-grappling-surge-banking-app-fraud-SABRIC/ (Accessed on 06 March 2024).

65. Patidar, R. & Sharma, L. 2021. Credit card fraud detection using neural network. *International Journal of Soft Computing and Engineering,* 1(2), pp. 2231-2307.
66. Pickett, K.S. and Pickett, J.M. 2002. *Financial crime investigation and control*. John Wiley & Sons.
67. Pieter, B. 2022. *Digital Transformation in South Africa's banking industry*. Available at: https://www.sovtech.co.za/blog/digital-transformation-in-south-africas-banking-industry (Accessed on 14 January 2023).
68. Prabakaran, M. 2014. *A Multi-Variant Relational Model for Money Laundering Identification using Time Series Data Set. Int. J. Eng. Sci*, 3, pp. 43–47.
69. PricewaterhouseCoopers. 2014. *PwC 2014 Global Economic Survey. Confronting the changing face of economic crime. 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2022).
70. PricewaterhouseCoopers. 2019. *PwC 2019 Global Economic Survey. Confronting the changing face of economic crime 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2022).
71. PricewaterhouseCoopers. 2020. *PwC 2020 Global Economic Survey. Confronting the changing face of economic crime 4th South African ed.* Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 16 June 2022).
72. PricewaterhouseCoopers. 2022. *Global Economic Survey. Confronting the changing face of economic crime 4th South African ed*. Available at: https://www.pwc.co.za/en/assets/pdf/global-economic-crime- (Accessed on 08 March 2023).
73. Priezkalns, E. 2019. *Mobile Money Fraud Advice Issued by GSMA*. Available at: https://commsrisk.com/mobile-money-fraud-advice-issued-by-gsma/ (Accessed on 23 March 2023).
74. 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 on 11 June 2023).
75. SABRIC. 2018. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).
76. SABRIC. 2019. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).
77. SABRIC. 2020. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).
78. SABRIC. 2021. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 14 April 2022).
79. SABRIC. 2022. SABRIC digital banking crime statistics. Available at: https://www.icfp.co.za/article/SABRIC-digital-banking-crimestatistics.html (Accessed on 23 August 2023).
80. Sekhu, K. 2023. Banking App kidnappings are on the rise in South Africa. Available at: https://www.kaya959.co.za/lineup/959-breakfast/banking-app-kidnappings-are-on-the-rise-in-south-africa / (Accessed on 12 March 2024).
81. Seleka, N. 2018. Minister Senzo Mchunu tells court how his SIM card was cloned to extort money from his contacts. News 24. April 21. Available at: https://www.news24.com/news24/southafrica/news/minister-senzo-mchunu-tells-court-how-his-sim-card-was-cloned-to-extort-money-from-his-contacts-20230421 (Accessed on 20 September 2023).
82. Sharma, A. & Panigrahi, P. K. 2013. A review of financial accounting fraud detection based on data mining techniques. *International Journal of Computer Applications*, 39(1), pp. 37 - 47.
83. Shulzhenko, N. and Romashkin, S., 2020. Internet fraud and transnational organized crime. *Juridical Tribune*, *10*(1), pp.162-172.
84. Snyder, H. 2019. Literature review as a research methodology: An overview and guidelines. *Journal of business research*, 104, pp.333-339.
85. Solin, M & Zerzan, A. 2010. Mobile Money: Methodology for Assessing Money Laundering and Terrorist Financing Risks. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2012/03/amlfinal35.updf. (Accessed on 18 February 2023).

86. Staff Reporter. 2023. Banking Apps are at the Centre of South Africa's Worrisome Abduction Surge. Available at: https://weetracker.com/2023/11/07/banking-apps-crime-south-africa/ (Accessed on 18 February 2023).
87. Sukhera, J. 2022. Narrative reviews: flexible, rigorous, and practical. *Journal of graduate medical education*, 14(4), pp. 414-417.
88. Sun, L., Srivastava, R. P. & Mock, T. J. 2016. An information systems security risk assessment model under the Dempster-Shafer theory of belief functions*. J. Manag. Inf. Syst*, 22, 109–142.
89. Thiel, D. 2016. *iOS application security: The definitive guide for hackers and developers*. No Starch Press.
90. Tobbin, P. 2021. Understanding mobile money ecosystem: ROLES, structure and strategies, in: *Mobile Business (ICMB),* 2021 Tenth International Conference on. IEEE, pp. 185–194.
91. Turvey, B. E. 2013. *Criminal Profiling.* Sitka: Elsevier.
92. Turvey, B.E. and Crowder, S., 2017. *Forensic investigations: An introduction*. Academic Press.
93. Wells, J.T., 2017. *Corporate fraud handbook: Prevention and detection*. John Wiley & Sons.
94. Welman, C., Kruger, F. & Mitchell, B. 2011. Research Methodology, 10th impression. In: I.I. Setlhodi (Ed). Values-Centered Leadership: Insights from Schools that Underperform. Oxford University Press.
95. Wewege, L., Lee, J. & Thomsett, M.C. 2020. Disruptions and digital banking trends. *Journal of Applied Finance and Banking*, 10(6), pp.15-56.
96. Yin, R.K. 2018. *Case study research and applications: Designs and methods (*6th edition). Los Angeles, CA: Sage.