

# Forensic Identification: The Biometric Technology Linked to Online Financial Fraud and Crime Related to the South African Banking Industry

Mokopane Charles Marakalala <sup>1</sup>

College of Law, School of Criminal Justice, Department of Police Practice, University of South Africa, Preller Street Muckleneuk Ridge, Pretoria, South Africa

<sup>1</sup> Corresponding author: [marakmc@unisa.ac.za](mailto:marakmc@unisa.ac.za)

© Authour(s)

OIDA International Journal of Sustainable Development, Ontario International Development Agency, Canada.

ISSN 1923-6654 (print) ISSN 1923-6662 (online) [www.oidaijsd.com](http://www.oidaijsd.com)

Also available at <https://www.ssm.com/index.cfm/en/oida-intl-journal-sustainable-dev/>

**Abstract:** This paper focuses on the forensic identification of the biometric technology linked to online financial fraud and crime related at the SABI. Biometric recognition, or biometrics for short, is the automatic identification of individuals based on their biological and behavioral characteristics. Due to the effectiveness of fingerprints in forensic science and law enforcement applications, as well as growing concerns about financial crime, cyber security, and border control, automated person recognition using fingerprints and other biological traits is becoming more and more common. Thus, it should come as no surprise that biometrics are used widely in many aspects of our society. Applications include border crossing, smartphone security, national civil registration, mobile payments, and restricted access. While many businesses have found success with biometrics, there are still a number of challenges to be solved and new opportunities for biometric person recognition. The quality of the generated biometric data may not be appropriate for automatic person recognition, particularly if the subject is resistant or the biometric data is obtained in an uncontrolled environment. It is likely that the biological evidence gathered from a crime scene is of low quality, which makes this especially true for crime-scene investigations.

**Keywords:** Forensic, Fraud, Investigation, Crime, Technology, Identification. Biometric, Financial, Cyber-Crime, Commercial Crime.

## Introduction and Background

This article first describes how forensic science gave rise to biometrics, then explores the field's historical foundations to address a few challenging problems. Biometric person recognition has shown promise in many industries, but there are still numerous challenges to be solved and opportunities for improvement (Akinbowale, Klingelhöfer, & Zerihun, 2020a; Ali, Ali, Surendran & Thomas, 2017:32). The resulting biometric data quality could not be appropriate for automated person recognition, particularly if the subject is resistant or the biometric data is gathered in an uncontrolled environment (Anonymous, 2019:np). This is particularly relevant to crime scene investigations since it is possible that the biological evidence that has been gathered from a scene is of poor quality. In order to address some challenging problems, this article first describes how biometrics evolved from forensic science. After discussing the similarities and differences between biometrics, the Association of Internal Control Practitioners (2024:np) will provide a few successful examples of how biometrics concepts are successfully applied to forensics to address urgent issues in the field of law enforcement.

According to Marakalala (2023:np), we finish by discussing possible collaboration opportunities for forensics and biometrics researchers in order to address outstanding issues that might benefit society as a whole.

In South Africa, identity fraud is still on the rise. The Southern African Fraud Prevention Service (SAFPS) reports that from April 2022 to April 2023, impersonation fraud rose by an astounding 356%. According to the statement made by Anonymous (2024:np), South Africa's current prelisted status has put pressure on the government and business to stop money laundering and financial fraud in its tracks, while the high-profile investigation into the citizenship of former Miss SA contestant Chidimma Adetshina has highlighted the social impact of false identity. There is also a growing concern that scammers may defraud customers of substantial quantities of money now that

the two-pot pension scheme went into effect on September 1. Employing a more potent type of defense—biometric digital identity—can halt these crimes in their tracks (Akinbowale, Klingelhöfer, & Zerihun, 2020b).

Global worry over online financial fraud is a serious issue (Girard, 2018:23). It entails using one's position for one's own gain by willfully misusing or stealing an organization's resources (Association of Certified Fraud Examiners 2023:np). According to the Banks Act (No. 94 of 1990) or the Mutual Banks Act (No. 124 of 1993), the South Africa Reserve Bank (SARB) is in charge of managing and overseeing the banking sector and financial institutions in the country. Its goal is to create a strong and effective banking system that serves the interests of both the economy and its clients (SARB, 2024:np). For most organizations, information technology (IT) is essential to doing daily tasks and reaching this goal (KMPG, 2019:np). But given that fraud, phishing, and hacking are all common in the banking sector, it can also be argued that IT has a negative effect on this sector (South African Reserve Bank, 2020:np).

#### **The main aspect of biometrics technology linked to online financial fraud and crime related**

- This paper focuses on the forensic identification of the biometric technology linked to online financial fraud and crime related.
- The automatic identification.
- Automated person recognition utilizing fingerprints and other biological features is becoming increasingly popular because to the efficacy of fingerprints in forensic science and law enforcement applications, as well as growing worries about financial crime, cyber security, and border control.
- Crime link to banking app kidnapping.




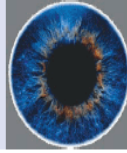
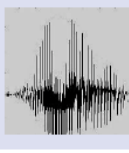
#### **Problem Statement**

The primary issue with this research is the need for more creative and safe banking methods that allow users to access their funds from anywhere at any time. With the advent of the fourth industrial revolution (4IR) and the demand for change in the banking industry, technology has given financial institutions more chances to take advantage of. On the other hand, a lot of financial institutions have adopted the conventional digital banking platforms as their operating model. Customers can monitor their accounts, make deposits, withdrawals, and transfers using this digital banking platform without having to visit the bank in person. However, none of these banking sectors have been able to take full advantage of the capacity and possibilities of the 4IR for a more innovative and simplified banking platform.

There aren't many research that focus on biometric payment and banking systems. In order to close the gap, this study uses biometrics to assess safe and creative ways to access money and pay for goods at retail establishments without using real cash or bank cards. The study focuses on biometrics as a digital banking financial technology substitute for authentication when doing mobile banking activities like bank transfers and payments. The authentication methods in use today still rely on traditional password authentication. Additionally, this article aims to raise awareness among banks and retailers of the critical role that biometrics play in providing a quick, secure, adaptable, and creative authentication process to safeguard customer funds and the organization, which may reduce or eliminate crime.

The layout of this article is as follows: the literature review portion covers the state of knowledge and research about biometric technologies in the banking industry. This research study aims to answer the research problem covered in section challenges of biometrics. The research technique is covered in section research method and design. The data analysis is finally covered in sections.

Biometric technology, which includes fingerprint readers, scanners, and facial recognition software, is widely used in everyday life for a variety of purposes, including smartphone unlocking, online banking, and sensitive government buildings. Forensic investigators explore the definition, uses, and wide range of methods and technology that make up this cutting-edge discipline of biometrics in this extensive reference (Michael-Kramer, 2018:np).

| BIOMETRIC                   | FINGERPRINT   | FACE  | HAND GEOMETRY  | IRIS  | VOICE   |
|-----------------------------|---|---|--|---|---|
|                             |  |  |  |  |  |
| Barriers to universality    | Worn ridges; hand or finger impairment  | None  | Hand impairment  | Visual impairment   | Speech impairment   |
| Distinctiveness             | High  | Low   | Medium   | High  | Low   |
| Permanence                  | High  | Medium  | Medium   | High  | Low   |
| Collectibility              | Medium  | High  | High   | Medium  | Medium  |
| Performance                 | High  | Low   | Medium   | High  | Low   |
| Acceptability               | Medium  | High  | Medium   | Low   | High  |
| Potential for circumvention | Low   | High  | Medium   | Low   | High  |

Source: Anonymous (2023:np)

**Research Aim and Objectives**

A research aim is a brief statement that encapsulates the primary goal or objective of a study effort. It provides a clear direction for the research's efforts and outcomes and lays out the study's overarching objective. Maxfield and Babbie (2021:19) offer a list of five different categories of research purposes, such as empowerment, description, explanation, and investigation, to help realise this unique vision. A deliberate, goal-directed, purposeful action carried out for a specific reason, such as (i) answering a specific question or query, (ii) fixing a problem, or (iii) addressing a specific issue or topic, is what Depoy and Gitlin (2016: 53) define as research. According to Denscombe (2018:98), it's typical to make a distinction between research, best practice development, analysis and criticism, and empowerment of others. Maxfield and Babbie (2021:19) offer a list of five different categories of research purposes, including empowerment, description, explanation, and inquiry, to help realize this unique vision. A deliberate, goal-directed, purposeful action carried out for a specific cause, such as the researcher's aim to: (i) address a specific question or query; (ii) address a problem; or (iii) address a specific argument or issue, is what Depoy & Gitlin (2016:53) define as research. Denscombe (2018:98); Leedy & Ormrod (2016:54) state that it is common to draw a line between research, best practice development, analysis and criticism, and empowerment of others. After considering the aforementioned concepts, the researcher determined that the aim of the study was:

- The aim of this paper is to explore the biometric technology linked to online financial fraud and crime related.

**Research objectives**

- To identify the biometric technology linked to online financial fraud and crime related;
- To identify challenges faced by Forensic Investigator: the biometric technology linked to online financial fraud and crime related;
- To develop new technologies for the biometric technology linked to online financial fraud and crime related.

**Methodology**

The research issue is addressed in the article using a qualitative research approach. Since this article addresses non-empirical topics, much of the material needed for it will be qualitative in character. This will assist the researcher in learning about biometrics technology that is connected to online financial fraud and crime that is relevant to the topic and is based on a real-life issue. Document review is typically the first step in the qualitative research process in order to gather data. A qualitative approach, in contrast to a deductive one, is subjective, value-laden, prejudiced, and inductive, claims Gordhan (2014:42). Through qualitative research, an investigator can assess the efficacy of current methods and obtain fresh perspectives on a phenomenon (Kumar, 2021:44). The goal and purpose of this paper are best served by a qualitative research design, which calls for the gathering of comprehensive data to investigate and comprehend the methods used by those who use biometrics technology in connection with online

financial fraud and other criminal activity (Holloway & Wheeler, 2013:77). Information about the use of biometric technology in online financial fraud and criminal activity will be gathered from a variety of sources, including pertinent national and international literature. The theory of an analysis of the modus operandi of perpetrators of biometrics technology linked to online financial transactions" will be explained through documentary sources.

### **Conceptual overview: biometrics technology linked to online financial fraud and crime related**

The ACFE (2023:np); Marakalala, (2023:np) outlined a number of biometrics technology linked to online financial fraud and crime related cases which was categorized and influenced by different categories, such as loss of revenue and fraudulent disbursement of cash (expenditures). The paper went on to emphasise that frequent detection techniques were categorized according to shifts in the methods of operation of those who used biometrics technology to commit online financial fraud and other crimes. These offenders comprised both external and internal employees (Mironov, & Zhuravskaya, 2016:np). The complex issue of biometrics technology with online financial fraud and crime stretches across a wide range of illegal actions, from bid rigging in the pre-contract award phase to fake invoicing in the post-contract award phase. Both people inside and outside of a SABI may commit it.

According to the ACFE annual report (2019–2023), it can be difficult to identify biometric technology used in online financial fraud and other criminal activity, and there have been few documented occurrences. It is therefore challenging to gauge the severity of the issue. Additionally, the necessary resources are directed toward document analysis to demonstrate the connection between biometrics technology and online financial fraud, crime, or irregularity, and to search for MO-specific similarities when biometrics technology is detected. Labuschagne (2015:53) defines modus operandi as a potentially dynamic method of identifying biometric technology associated with online financial fraud and criminal activity. The statement by Modugu and Anyaduba, (2013:65), identification of biometrics technology linked to online financial fraud and crime related is reliant on the collection of evidentiary material to determine the modus operandi and possibly the identity of the perpetrator which remains at the precipice of any documentary analysis in biometrics technology linked to online financial fraud and crime related (Marakalala, 2023:np).

The method of operation of those who use biometrics to commit crimes connected to the SABI and internet financial fraud is assessed in this article. The research goal and the implications of individualization and identification, together with the application of modus operandi as an identification approach, are the main topics of this work. There is discussion of the idea of fraud as well as a number of theories, including those that look at the methods used by offenders and the variables influencing those methods. Lastly, MO of the offenders in SABI is examined in this work.

### **Historical overview of forensic identification on the biometric technology linked to online financial fraud and crime related**

The most crucial elements of historical research are finding the unknown or filling in the gaps left by earlier researchers, responding to inquiries, determining the connections between the past and the present, documenting and evaluating individual accomplishments, and promoting an awareness of our own culture (Korrapati, 2016:76). According to Turvey (2013: 311), historical events pertaining to MO include methods that date back to 1809, when law enforcement officials looking into white collar crimes, such as biometrics technology linked to online financial fraud and crime related, believed that the best way to look into and eventually catch offenders was to understand their methods of operation (Marakalala, 2023:np).

The greatest investigating officers have historically been expected to become living encyclopedias of criminal cases and habits in order to employ MO information. The fundamentals of analysis hold true whether analyzing modus operandi information through basic analysis or advanced technological analysis, for example the manual processing of MO entails the systematic manual analysis of daily reports of serious biometrics technology linked to online financial fraud and crime related by way of:

- *Determining the location;*
- *Time;*
- *Unique characteristics;*
- *Similarities to other criminal events;*
- *Various significant facts that may help to identify either a criminal, or the existence of a pattern of criminal activity.*

However, technology has made it possible to use complex software, such as frequency charting, notebook analysis, data correlation, and link analysis, to plot, map, and link offenders to a particular time, location, and date as well as to several biometric technologies connected to online financial fraud and other types of crime.

### **Conceptualisation of *Modus Operandi* in the biometrics technology linked to online financial fraud and crime related**

Turvey (2013:145) claims that the term MO, which refers to the way biometrics technology is connected to online financial fraud and crime related, is Latin and denotes a technique of identifying. According to Labuschagne (2015:125), the investigation and preservation of a perpetrator's MO have historically been important for the following reasons:

- Analysing linkage of unsolved cases by MO.
- Data collection of evidence to identify perpetrator's MO with biometrics technology linked to online financial fraud and crime relateds committed or unsolved cases.
- Routine comparison of arrestee MO with the MO evident in unsolved cases.
- Development of investigative leads and suspect identity in unsolved cases by accumulating MO information.
- Offender prioritisation and elimination.
- Clearance of repeated biometrics technology linked to online financial fraud and crime related cases.
- As a technique for perpetrator identification, to bring about the identification and detection of criminals,
- As an aid in the prevention of biometrics technology linked to online financial fraud and crime related,
- As an aid in the questioning of suspects, and
- In the place of investigating personnel and resources in places where observation is required.

According to Murray (2024:56), the perpetrator's activities during the use of biometric technologies connected to online financial fraud and criminal activity are known as the MO. The authors continue by describing MO as a set of taught behaviors that criminals have picked up and adhere to because they are effective, but they also acknowledge that MO was adaptable and dynamic (Garger, 2014:12). They maintain that the criminal's method of operation would always change along with him or her, regardless of the situation. Documentary record manipulation and misrepresentation, frequently through forgery or counterfeiting, were a substantial component of MO in biometrics technology associated to online financial fraud and criminal related cases (Davis & Pesch, 2013:32). Additionally, the author suggests that detectives will benefit from knowing the MO because it will provide a helpful point of reference for where to concentrate their efforts. According to Cieslewicz (2018:78), the following instances of MO data in biometrics technology connected to analyses of crime and online financial fraud could include:

- Place, date and time of the biometrics technology linked to online financial fraud and crime related;
- Location of offence;
- Age of the victim;
- Number of offenders;
- Amount of planning before a biometrics technology linked to online financial fraud and crime related;
- Type of targets;
- Techniques and instruments to be used;
- Methods of committing the biometrics technology linked to online financial fraud and crime related;
- Language used;
- Nature and extent of precautionary acts;
- Type of transportation used to and from the biometrics technology linked to online financial fraud and crime related scene;
- Items taken from the victim or biometrics technology linked to online financial fraud and crime related scene(s).

According to Price Waterhouse Coppers' Global Economic Crime Survey (2016:np), there are a number of biometric technology types that have been connected to crimes and online financial theft. The paper lists some of the more typical instances of internal fraud, including:

#### **Payments:**

A side payment occurs when two parties to a transaction exchange money that wasn't needed for the transaction itself. Usually, its purpose is to persuade the recipient to participate in the transaction (Brytting, Minogue & Morino, 2018:66). Some instances of these payments are as follows:

- False charging of personal expenses;
- Double payments against single transaction;
- Inclusion of dummy workers in wage bill;
- False credit to various personal accounts for withdrawal later;
- The method used to commit the fraud; financial documents falsified by the perpetrator to conceal the fraud;
- Details of suppliers over charging for goods in collusion with employees;
- Details of payments effected with no supporting documents and details of personal purchases made on the business account.

#### **Manipulation of accounts**

In order to deceive investors and other users of this information, manipulating accounts entails breaking the law to change the meaning of the financial statements. Buckles (2017:88) cites the following instances of account manipulation:

- Under valuation of stock;
- Over valuation of stock;
- Fictitious purchase;
- Wrong allocation of revenue and capital expenditure;
- Recording next year's revenue as income for current period as income for current period, overstatement of profit or understatement of profit and over or under invoicing.

#### **Misappropriation of goods & services:**

According to Dzumira (2017:43), misappropriation of assets is the real theft of property belonging to an entity. This can be done by regular thievery or by tricking an organization into paying for products and services that they haven't really got (like phony suppliers or workers). The report also emphasizes asset misappropriation and fraudulent financial reporting, two distinct forms of internal fraud (Girard, 2018:89; James, & Nordby, 2018:28). Misappropriation of assets involves the actual theft of an entity's assets. This can be accomplished by common theft or the following:

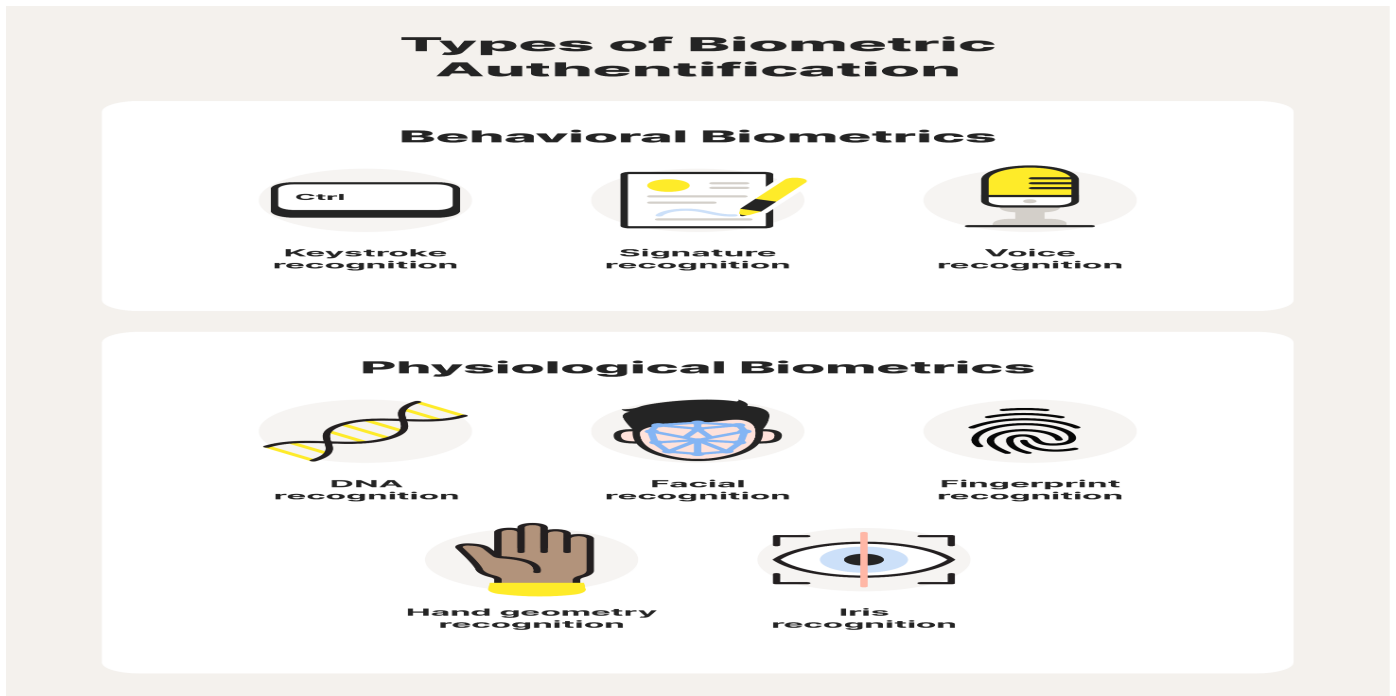
- Causing an organization to pay for goods and services not actually received (for example fictitious vendors or employees);
- Using an organization's assets for personal use;
- Embezzling receipts.
  - Omitting to enter goods received;
  - Recording less quantity than received;
  - Recording excess issue than actually issued;

#### **Procurement of low-quality goods:**

Labuschagne (2015:288) cites Esteves and Barclay (2018:76) as saying that MO is the "habits and techniques of criminals who have become stereotyped." "Routine mode of conduct in which individualised techniques are employed" is how he sees it. MO can be defined as a conglomeration of offenders' routines, tactics, and peculiar behavioral patterns that they tended to adhere to and rarely strayed from (Evans, 1987:90; Van Rooyen, 2017:15). According to the ACFE reports (2019/2023) and the SABIC annual report (SABRIC, 2019/2023), offenders of biometrics technology linked to online financial fraud and crime have certain habits, tactics, and behavioral patterns. These include the following:

- Conflict of interest situation;
- Nonexistent company whose invoice is presented by an official involved in purchase process;
- Excess purchases with a view to divert for personal use;
- Split purchases to evade competitive bidding in exchange of favours;
- Extortion;
- Nepotism;
- Tax or duty evasion through false representation involving negligence of government officials.

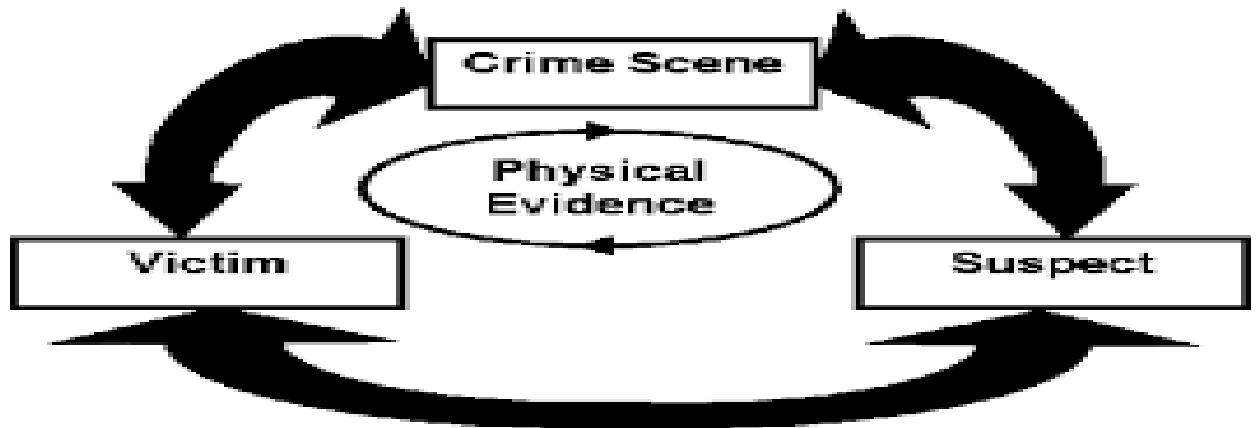
Comprehending the behaviors and methods employed by those involved in biometric technology-related online financial fraud and criminal activity is essential as it offers valuable insights to the investigator into the methodology. The offender's MO information is crucial for examining biometric technology connections to online financial fraud and criminal activity.



Source: Anonymous (2023:np)

### **Locard's exchange principle applied in tracing the perpetrator of online financial fraud and crime related**

In order to recreate and characterise previous events in a legal framework, forensic science applies scientific concepts to the analysis of evidence found at crime scenes. Locard's exchange theory, which argues that a criminal would bring something into the crime scene and take something with them, both of which can be utilized as forensic evidence, has had a significant influence on it.



Source: Anonymous (2023:np)

### **The value of perpetrator modus operandi in biometrics technology linked to online financial fraud and crime related**

The method of operation of known offenders and the method used in previous biometrics technology linked to online financial fraud and crime related by unidentified criminals are both valuable information found in modus operandi information and, in particular, records (Hess & Orthman, 2013:324 and Rustiarini, Nurkholis, & Andayani, 2019:36, Marais and Van Rooyen, 1990:34 and Van der Westhuizen, 1996:33). Whether on arrest cards or in computer databases, Turvey (2013:407) and Rustiarini, Nurkholis, and Andayani (2019:36) are certain that modus operandi must be gathered, recorded, and analyzed. The authors also state that the advantages of recording modus operandi information include:

- Linking of unsolved biometrics technology linked to online financial fraud and crime related;
- Developing of investigative leads;
- Prioritizing perpetrator identification or elimination of perpetrators;
- Clearing of unsolved cases.

According to Casey (2018:256), it is important to recognize that biometric technology has been connected, through documented or recorded behavioral modus operandi information, to incidences of online financial fraud and criminality. He contends that given the lack of tangible proof and witness accounts, recorded behavioral modus operandi information is essential.

Installing biometric systems is made easier, of course, by growing public acceptance, significant accuracy advances, a rich offer, and declining costs for sensors, IP cameras, and software. These days, a lot of applications employ this technology.



Source: Anonymous (2023:np)



They can be either morphological or biological.

- Morphological identifiers mainly consist of fingerprints, the hand's shape, the finger vein pattern, the eye (iris and retina), and the face's shape.
- For biological analyses, DNA, blood, saliva, or urine may be used by medical teams and police forensics.

### Literature review

Insofar as they usually appear in specific formats, such as notes, case reports, contracts, drafts, death certificates, remarks, diaries, statistics, yearly reports, certifications, verdicts, letters, or expert views, documents are considered "consistent artefacts." The researcher analyzed case files with the goal of determining the biometric connections to connected crimes, which helped to establish the study's credibility. The Biometrics case files have connections to related crimes.

The stated economic crime rate in South Africa as of 2024, compared to the average rate worldwide (PwC's Global Economic Crime Survey, 2024:np). In comparison to its top spot in 2018 (PwC's Global Economic Crime Survey, 2024:np; PwC's, 2018:np), South Africa was placed third among the ten nations with the highest reported rates of economic crime worldwide. This suggests a 17% drop in the estimated global rate of economic crime between 2018 and 2024. (World Economic Crime Survey, PwC, 2024:np). When compared to other nations, this suggests that between 2018 and 2024, South Africa's recorded economic crime rate declined little. The prevalent economic crime in South Africa has been identified as customer's fraud, bribery and corruption, financial statement fraud and cybercrime (PwC's Global Economic Crime Survey, 2024:np). The PwC's Global Economic Crime Survey (2024:np) categorised fraud perpetrators into three categories: external perpetrators, internal perpetrator as well as collusion between external and internal perpetrators. According to PwC's Global Economic Crime Survey, 2024:np, the largest percentage of offenders—41 percent—are internal, followed by external perpetrators (36%). Collusion between internal and external perpetrators accounts for the remaining 21% of reported economic crime rates in South Africa.

### Results and discussions

This paper explains how biometrics developed from forensic science and then goes back to its roots to solve some difficult issues. Although, biometrics has been successfully used in many industries, there are still a number of obstacles to overcome and new prospects for biometric person recognition. Especially if the individual is recalcitrant or biometric data is collected in an unrestricted setting, the resulting biometric data quality could not be suitable for automated person recognition.

#### Aspect of Biometrics technology links to online financial fraud and related crime:

- Forensic biometrics technology involves the use of unique identifiers, such as fingerprints, DNA, and facial recognition, to solve crimes.
- These identifiers can be used to identify suspects, link suspects to crime scenes, and exclude suspects from investigations.
- The use of biometrics in forensic science has greatly improved the accuracy and efficiency of criminal investigations.

#### The forensic identification of the biometric technology linked to online financial fraud and crime related.

Previous research has linked the latest technological advancements and innovations in this digital age to one of the main causes of the online financial fraud and crime related and the rising risk of it in South Africa (Dlamini and Mbambo, 2019:1; Herselman and Warren, 2004:263; Dzomira, 2017:143; Coetzee, 2018:3; Dagada, 2013:148; Sutherland, 2017:84). According to UK Finance (2018:6), cybercriminals have used a variety of tactics to influence financial institutions over time, including phishing emails, impersonation, and account hacking. This has made it possible for unauthorized individuals to obtain private information and compromise financial institutions. Similarly, Dzomira (2014:16) explained that the banking industry in Zimbabwe has also suffered cyberfraud different forms such as unauthorised intrusion into the banks or personal information or accounts, credit/debit card fraud, money laundering, employee embezzlement, pharming, phishing, malware, hacking, virus, spam and advance fee fraud.

To mitigate cyberfraud occurrences, Akinbowale *et al.* (2024a:np) recommended that anytime there is unauthorised access to a financial institution's database or a customer's account, real-time alert systems that can notify the financial institutions and their clients of the situation should be used. This will improve the ability to stop such intrusions quickly before any unauthorized transactions happen. Two simplified conceptual models for cyberfraud

mitigation have also been reported by Akinbowale et al. (2024b:np). While the second model covered the thorough investigation and extensive data analysis methods of identifying fraud, the first model addressed the integration of forensic accounting into the organization's structure.

This will improve the organization's control framework and facilitate the investigation and mitigation of fraud. This is due to the fact that the model includes all of the procedural processes involved in implementing forensic accounting, including the first survey, in-depth investigation, thorough data analysis, reporting, and expert witness. Dzumira (2017:143) recommended that internet banking consumers be made more aware of the types of cyberfraud that are committed by hackers in South Africa, as well as the necessity of strengthening cyberfraud alert systems. Although information regarding Internet banking fraud was available on the websites of South African banks, this report recommended raising awareness about the types of cyberfraud and how they were carried out. The banking industry should actively combat online banking fraud, according to Dzumira (2017:150), in a way that benefits its customers and the country's many communities.

### **The automatic identification**

Due to the effectiveness of fingerprints in forensic science and law enforcement applications, as well as growing concerns about financial crime, cyber security, and border control, automated person recognition using fingerprints and other biological traits is becoming more and more common.

#### *Identity as a human right*

According to Anonymous (2023:np), having a legitimate digital identity lets people be more inclusive regardless of their gender, geography, or level of education. Undocumented residents of South Africa face limitations on their capacity to access healthcare facilities and receive social handouts. Because of lengthy and ineffective identification procedures, even people with legal IDs must wait in line for hours.

Systemic inequality and the sluggish adoption of modern digital technology, which should be extensively employed to reduce inequality, are major causes of South Africa's problems. The maintenance of identities is significantly impacted by this disparity in access. Because of this, having the ability to prove one's identification is a fundamental human right rather than merely a bureaucratic process (Anonymous, 2023:np).

A verified identity that can be verified is a necessary step in every process, including applying for legal work, setting up an address, acquiring or buying a phone contract, and creating a bank account (Anonymous, 2023:np). Digital identity that is widely used and reliable benefits both citizens and governments as well as financial institutions.

#### *The case for face biometrics in confirming a person's identity*

It is conceivable and continues to occur to impersonate someone using physical paperwork, as was the case with Chidimma Adetshina. These days, even conventional verification techniques like fingerprints and OTPs are insufficient. Cybercriminals are merely using technology that is developing too quickly. With the use of deepfake technology, fraudsters may even mimic a person's voice. Due to its ease of use and widespread consumer familiarity, face biometrics are the most effective biometrics currently available on the African continent. The majority of individuals feel at ease taking selfies, and they may now utilize such verified selfies to gain access to important services. By comparing these selfies to a reputable or official database, 4D Liveness technology can be used to authenticate them.

In a nutshell, proof of liveness is the affirmation and verification that a genuine, living person is on the other end of a gadget, carrying out a transaction. It is harder to create a sense of biometric human life, even though thieves can mine personal data and use targeted attacks to take over certain systems. "The rise of identity theft is concerning, but it is a challenge that can be solved with the right technology," the statement continues. As a reputable technology supplier in this field, we are witnessing an increasing need on the part of both government agencies and corporations to collaborate in order to give individual identity security first priority and, as a result, significantly lower the number of identity-based crimes.



Source: Anonymous (2024:np)

### **Crime link to banking app kidnapping**

Investigations into abduction-related complaints filed with the NFO have revealed that, following their kidnapping and detention, criminals threaten and use violence to coerce banking customers into disclosing their online banking and banking app passwords (Anonymous, 2023:np). Banks' implementation of many security layers on their online platforms may be one reason fraudsters are resorting to this new method of operation. These steps are making it harder and harder for scammers to get private banking information from banking clients.

"After kidnapping and detaining the victim, criminals use threats of violence (duress) to coerce the victim into disclosing their online banking and banking app passwords," according to complaints about kidnapping that have been reported to the NFO. According to Maseti see (Anonymous, 2023:np), if criminals obtain access to these platforms, they can change account restrictions and make unauthorized transfers, which can result in severe financial losses in addition to the anguish of the kidnapping itself.

Maseti emphasises that it's critical to comprehend the NFO's objectives before delving into banking issues. The NFO's main goal is to look into and address consumer complaints against financial service providers in the credit, banking, and insurance (both life and non-life) sectors.

"The NFO's banking division thoroughly investigates each case when a customer files a complaint about losses incurred as a result of the forced disclosure of private banking information after a kidnapping, and the resolution is based on the merits of each individual matter." Investigating such complaints usually entails determining if the bank committed any misconduct or negligence that resulted in or contributed to the customer's losses (Anonymous, 2023:np). The NFO's banking division is empowered to advise the implicated bank to reimburse the part of the customer's losses that could have been avoided but for the bank's actions if an inquiry reveals that the bank could have prevented or lessened the customer's losses but chose not to do so. The NFO, an independent organization, is steadfast in its resolve to settle conflicts fairly and without charging the complainant. (Anonymous, 2023:np) claims that the NFO makes sure banks handle their clients properly and in accordance with their own policies, procedures, and any relevant laws, rules, and conduct codes.

### **Case study**

*According to a recent inquiry, a complainant was abducted and coerced into disclosing their internet banking login details, which led to R103 092 in unauthorized transactions. After being notified of the activity on the complainant's accounts by the bank's fraud monitoring system, the complainant verified the legitimacy of the payments (under duress). Following their release, the*

*complainant went to the bank to report the occurrence and requested a complete refund. Citing the complainant's disclosure of their private banking information, the bank denied the claim.*

*"The parties' contract was taken into consideration throughout the NFO's examination. According to the contractual terms and conditions of the bank's online banking platform, a client is responsible for all transactions made before the bank is informed of any unauthorised or fraudulent activity if a third party obtains access to their online banking profile. Regretfully, before the bank was informed of the event, all of the money that had been moved out of the complainant's accounts had already been used. As a result, the bank was not judged to have been careless in minimizing the complainant's loss. We could not legally hold the bank accountable for the complainant's loss given the merits of this case. In essence, the complainant was a victim of a crime that had no connection to the bank. But as a gesture of goodwill, the bank consented to reimburse a portion of the loss, at its business discretion, according to Maseti.*

Customers of banking institutions are typically held accountable when they divulge their private banking information. However, as soon as the compromise is disclosed, the bank becomes liable. The bank is required to minimize any losses after being notified (Anonymous, 2023:np). Every case must be evaluated on its own merits, and the NFO's conclusions are based on the particular facts of each case. If the customer is found to be at fault, the bank may still take into account their unique situation and susceptibility and, in some situations, provide a partial refund as a courtesy. Maseti highlights that this is a complex topic with many factors to take into account (Anonymous, 2023:np). The challenging issue for banks is to verify the alleged criminal claims and that the private data was, in fact, tips for prevention and mitigation:

- With this type of crime increasing, consumers can take a few measures to protect themselves and mitigate significant damages. The tips identified below are similar to those for any hijacking risks.
- *Be cautious when posting online.* Avoid posting sensitive financial information or sudden changes on social media. It is extremely important to be vigilant about what information share on social media and the perceptions to create about yourself, family, and friends. Avoid posting about sudden influxes of funds, as this can make person a target for criminals.
- *Do not draw unwanted attention to yourself.* Wearing expensive jewellery, carrying high-end branded items, or carrying other valuables in public may attract unwanted attention.
- *Vary a daily routine as often as possible.* Diversify a daily activity to reduce predictability. Criminals may monitor predictable routines well before the actual crime is perpetrated in order to ensure that they are vulnerable to criminal targeting.
- *Consult with the bank.* Discuss the measures of the bank may offer to help mitigate potential losses if become a victim of any type of banking fraud. Many banks provide options to tailor online banking and app experience, including limiting exposure and risk.
- *Consider investment options.* Use accounts with restricted access to limit potential losses. In some instances, investing in a notice account may reduce access to funds, thereby limiting your overall loss.
- *Consider insurance.* Check if the bank offers duress insurance or trauma counselling services. These may help in tough situations.

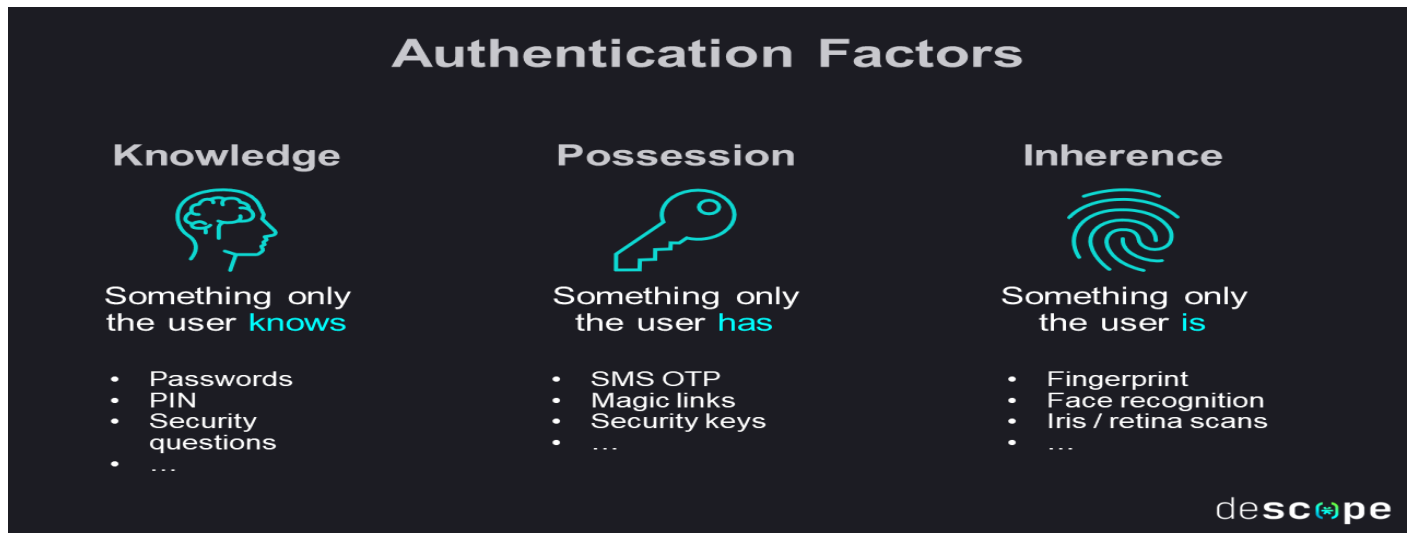
Finally, consumers are urged to remain vigilant and to take proactive protective measures. According to Van Graan, & Budhram, (2015:33) if a bank client fall victim to such crimes, report the incident to the SAPS and the relevant law enforcement agencies to investigate and prosecute the perpetrators of the crime,"

### **Research Findings**

This paper presents the interpretation of the research findings. The information obtained through the process of documentary analysis or case files were explore and presented by means of the emerging themes in the previous chapter. This was done in order to present a detailed discussion of the biometric technology linked to online financial fraud and crime related in South Africa Banking Industry. Findings refer to results that were discovered during the research. The aim of non-empirical data collection with representatives of the biometric systems

providers and experts was to learn more about the current state of biometrics systems in the South African Banking Industry and to explore opinions about attitudes and factors influencing adoption/deployment of biometrics systems in the banking sector. In this research, to express their experiences, opinions and domain knowledge about the implementation of the biometric technology linked to online financial fraud and crime related in South Africa Banking Industry.

- Develop efficient Morphing Attack Detection (MAD) solutions that are suitable for enrolment, forensic investigation, and online financial crime.
- Develop a prototype demonstrator for Document Verification and Fraud Detection (DVFD) tools.
- Assess vulnerabilities in biometric systems, notably against morphing attacks.
- Anticipate new morphing attacks against face images and other biometric modalities for future travel documents.
- Train people involved in online financial application, delivery, and checks to increase their ability to detect OFC.
- Standardize Presentation Attack Detection (PAD) and face image quality assessment.
- Provide open access benchmarks to research activities on OFC.
- Ensure that new technologies developed.



Source: Anonymous (2024:np)

### Recommendations

Incorporating ‘privacy by design’ and implementing best practice of the biometric technology linked to online financial fraud and crime related in South Africa Banking Industry frameworks to strengthen systems will act as a barrier to identity theft. Increasing collaboration among industry players to share near real-time information on data breaches and related incidents (subject to data privacy laws) will limit the scale of losses as a result of identity thefts. Proactively educating customers on the latest techniques being used by fraudsters to steal identity information will alert customers to not reveal personal information. Reporting data breaches (providers) and identity theft (customers) immediately to law enforcement agencies will limit exposure. Identity theft is a common prerequisite to other serious unlawful activities such as fraudulent SIM swaps (ACFE, 2023:np). To mitigate the risks of identity theft and associated frauds, it is important to look at these frauds in tandem, as one often leads to another (Zinn & Dintwe, 2015:65).

The purpose of this paper is to investigate biometric-based methods for preventing mobile fraud in the banking sector of South Africa. The paper also sought to investigate biometric-based solutions for thwarting mobile fraud, according to ACFE (2023:np). A qualitative methodology was employed in the gathering and investigation of non-empirical data. The outcomes of the non-empirical data analysis and the literature research showed that the gathering and management of digital evidence played a significant role in determining whether mobile fraud succeeded or failed.

The statement by Marakalala (2023:np) recommended that:

- This is especially true for crime-scene investigations, because it's possible that the biological evidence collected from a scene is of low quality.
- This article first explains how biometrics developed from forensic science and then goes back to its roots to solve some difficult issues.
- The parallels and distinctions between biometrics will then be discussed, followed by a few examples of successful applications where biometrics concepts are effectively used to forensics to resolve pressing issues in the field of law enforcement.
- In order to address unresolved issues that might benefit society as a whole, the researcher conclude by talking about potential cooperation prospects for biometrics and forensics researchers.

## Conclusion

In conclusion, biometrics are a crucial component of contemporary security procedures because they provide improved security, convenience, and dependability in a variety of settings, as well as enable regulatory compliance and technological advancements. However, biometrics are linked to related crimes.

Law enforcement's capacity to solve crimes and apprehend offenders has been substantially improved by the application of biometric and access control in forensic science. In order to effectively limit the effects of online financial fraud and crime related, the purpose of this study is to evaluate the forensic identification in the biometric technology associated to online financial fraud and crime related in the banking industry in South Africa. A qualitative strategy utilizing case files or documentary analysis was used to accomplish this. In all, fifteen documentation analyses from the secondary data collection were acquired. The findings showed that the South African banking sector is significantly impacted by online financial fraud and crime, and that these incidents have a negative impact on the sector's reputation in terms of revenue loss, productivity loss, reputation loss, and shareholder loss (Taroni, Bozza, Biedermann, Garbolino, & Aitken, 2010:32).

According to the results obtained, the prevalent forms of online financial fraud and crime related perpetrated in the South African banking industry include phishing, spying, malware, data theft, spam e-mail, online theft, hacking and skimming. Hence, a holistic review of the internal control system of the banking structure is hereby recommended. Online financial fraud and crime related had been reported to have negative impact on an SABI's profitability, customers' satisfaction, public trust, SABI good will and risk management globally. This calls for the need to review the diverse ways of curbing online financial fraud and crime related to lessen its impact or associated fraud risks on the banking operation (SABI for Economic Co-Operation and Development., 2016:np).

This paper provides non-empirical findings that could assist the South African banking industry in the areas decision making or policy formulation geared towards of online financial fraud and crime related mitigation. This research notifies the South African banking industry about the nature of online financial fraud and crime related perpetrated (Singleton & Straits, 2010:98). The understanding of the nature of online financial fraud and crime related perpetrated can assist the South African banking industry to formulate measures to mitigate them. The findings reported in this paper is based on the views of the forensic identification in the biometric technology linked to online financial fraud and crime related in South Africa consulted as well as those of the SABIs. Future works can consider the analysis of the level of effectiveness of the fraud control measures in the South African banking industry vis-a-vis the forms of the biometric technology linked to online financial fraud identified.

## List of Reference:

- Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020a), "Analysis of cyber-crime effects on the banking industry using balance score card: a survey of literature", *Journal of Financial Crime*, Vol. 27 No. 3, pp. 945-958.
- Akinbowale, O.E., Klingelhöfer, H.E. and Zerihun, M.F. (2020b), "An innovative approach in combating economic crime using forensic accounting techniques", *Journal of Financial Crime*, Vol. 27 No. 4, pp. 1253-1271.
- 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*, Vol. 29 No. 3, pp. 884-1008.
- Albrecht, C., Holland, D., Malagueno, R., Dolan, S. and Tzafirir, S. (2015), "The role of power in financial statement fraud schemes", *Journal of Business Ethics*, Vol. 131 No. 4, pp. 803-813.

- Ali, L., Ali, F., Surendran, P. and Thomas, B. (2017), "The effects of cyber threats on customer's behaviour in e-bankingservices", *International Journal of e-Education, e-Business, e-Management and e-Learning*, Vol. 7 No. 1, pp. 70-78.
- Anonymous, 2019. Property 24. R100-million fraud alleged. Available at <https://www.property24.com/articles/r100-million-tender-fraud-alleged/13278> (Accessed 10 July 2024)
- Anonymous (2023:np) Biometrics is the most suitable means of identifying and authenticating individuals in a reliable and fast way through unique biological characteristics. Available at: <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics> (Accessed on 04 September 2024)
- Anonymous. 2023. Face biometrics offers critical first line of defence against rising identity fraud in SA: Available at: [Face biometrics offers critical first line of defence against rising identity fraud in SA - South African Business Integrator \(sabusinessintegrator.co.za\)](https://www.sabusinessintegrator.co.za) (Accessed on 04 September 2024)
- Anti-Intimidation and Ethical Practices Forum (AEPF) (2020), "Unpacking fraud", pp. 1-9, [Online], available at: [www.aepf.co.za/Unpacking\\_Fraud.pdf](http://www.aepf.co.za/Unpacking_Fraud.pdf) (Accessed on 16 November 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](http://www.acfe.com/uploadedFiles/ACFE_Website/Content/resources/Benchmarking_Technology_Report.pdf) (Accessed on 2 December 2024).
- Association of Certified Fraud Examiners (ACFE) (2020), "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](http://www.acfe.com/uploadedfiles/acfe_website/content/european/course_materials/2012/11c_risch-cpp.pdf) (Accessed on 2 February 2024).
- Association of Internal Control Practitioners. (2024), "Combatting Biometrics technology linked to online financial fraud and crime related", available at: <https://www.theaicp.org/combating-procurement-fraud/> (accessed 20 January 2024).
- Babbie, E. & Mouton, J. 2018. *The practice of social research*. Cape Town: Oxford University Press.
- Babbie, E. 2018. *The practice of social research*. Belmont: Wadsworth.
- Bennett, W. W. & Hess, K. M. 2017. *Criminal Investigation*. 8th edition. Belmont: Wadsworth/Thomson Learning
- Benson, M.L., Madensen, T.D. and Eck, J.E. (2009), "White-collar crime from an opportunity perspective", *The Criminology of White-Collar Crime*, Vol. 3, pp. 175–193.
- Blackburn, K., Bose, N. and Haque, M. E. (2018), "Public expenditures, bureaucratic biometrics technology linked to online financial fraud and crime related and economic development", *The Manchester School*, Vol. 79 No. 3, pp. 405–428.
- Blackburn, K., Bose, N. and Haque, M.E. (2018), "Public expenditures, bureaucratic corruption and economic development", *The Manchester School*, Vol. 79 No. 3, pp. 405–428.
- Bolton, C. 2016. Public Procurement. 2015. *SA public procurement: poor value for money*. Available at: [www.smartprocurementworld.com](http://www.smartprocurementworld.com) (Accessed on: 28 October 2018).
- Brown, L. & Holloway, I. 2013. *Qualitative Research in Sport and Physical Activity*. SAGE Publications Ltd
- Brytting, T., Minogue, R. and Morino, V. (2018), *The Anatomy of Fraud and Corruption: Organizational Causes and Remedies*, Gower Publishing, Ltd.
- Buckles, T. 2017. *Biometrics technology linked to online financial fraud and crime related Scene Investigation: Criminalistics and the Law*. New York: Thomson Delmar Learning.
- Burchell, J. M. 2013. *Principles of Criminal Law*. (4<sup>th</sup> Edition). Cape Town. Juta.
- Caulfield, T. and Steckler, S. (2014), "The five faces of biometrics technology linked to online financial fraud and crime related, abuse, and noncompliance", *Contract Management*, Vol. December, pp. 38–45.
- Cieslewicz, J. K. (2018), "The fraud model in international contexts: A call to include societal-level influences in the model", *Journal of Forensic & Investigative Accounting*, Vol. 4 No. 1, pp. 214–254.
- Creswell, J. W. 2014. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches*. (4<sup>th</sup> Edition). Thousand Oaks: Sage.
- Davis, J. S. and Pesch, H. L. (2013), "Fraud dynamics and controls in organizations", *Accounting, Organizations and Society*, Vol. 38 No. 6–7, pp. 469–483.
- Denscombe, M. 2018. *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*. (5<sup>th</sup> Edition). USA: Elsevier
- Dorminey, J., Fleming, A. S., Kranacher, M. and Riley, R. A. (2010), "Beyond the fraud triangle", *fraud triangle*", *Accounting Forum*, Vol. 37 No. 1, pp. 29–39.



- Dzomira, S. (2017), "Internet banking fraud alertness in the banking sector: *South Africa*", *Banks and Bank Systems*, Vol. 12 No. 1, pp. 143-151.
- Esteves, A. M. and Barclay, M. A. (2018), "Enhancing the benefits of local content: integrating social and economic impact assessment into procurement strategies", *Impact Assessment and Project Appraisal*, Vol. 29 No. 3, pp. 205–215.
- Evans, E. (1987), "Fraud and incompetence in purchasing", *Industrial Management & Data Systems*, Vol. 87 No. 3/4, pp. 25–27.
- Garger, J. 2014. *Common Latin Phrases 'Modus Operandi, Deus ex Machina, and Curriculum Vitae'*. Available at: <https://www.brighthubeducation.com/learning-translating-latin/40674-common-latin-phrases-modus-operandi-deus-ex-machina-and-curriculum-vitae/> (Accessed 11 December 2023).
- Girard, J. E. 2018. *Criminalistics: Forensic Science and Biometrics technology linked to online financial fraud and crime related*. Burlington: Jones and Bartlett.
- Gray, D. E. 2014. *Doing research in the real world*. London: SAGE.
- Holloway, I. and Wheeler, S. 2013. *Qualitative Research in Nursing and Healthcare*. (3<sup>rd</sup> Edition). UK: Wiley-Blackwell, A John Wiley & Sons, Ltd.
- James, S. H. & Nordby, J. J. 2018. *Forensic science. An introduction to Scientific and Investigative Techniques*. 3<sup>rd</sup> edition. Boca Raton: CRC Press.
- KMPG (2019), "The Multi-Faceted threat of fraud: are banks up to the challenge?", *Global Banking Fraud Survey*, [Online], available at: [www.kpmg.com](http://www.kpmg.com) (Accessed on 5 May 2024).
- Kroll. (2013), "2013/14 Global Fraud Report", available at: <http://fraud.kroll.com/introduction/> (accessed 21 March 2024).
- Kumar, R. 2018. *Research Methodology- a step-by-step guide for beginners*. (3<sup>rd</sup> Edition). London: SAGE Publications.
- Kumar, R. 2021. *Research Methodology. A step-by-step guide for beginners*. (4th ed). London: SAGE.
- Labuschagne, G. 2015. *Criminal Investigative Analysis: An Applied Perspective*. In Zinn, R.J. & Dintwe, S.I. (eds) 2015. *Forensic Investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta.
- Leedy, P.D. & Ormrod, J.E. 2016. *Practical Research: Planning and Design*. (11<sup>th</sup> New Jersey): Pearson Education International.
- Lochner, H.T. & Zinn, R.J. 2015. *Crime Scene Investigation*. Claremont: Juta.
- Lokanan, M.E. (2015), "Challenges to the fraud triangle: Questions on its usefulness", *Accounting Forum*, Vol. 39 No. 3, pp. 201–224
- Marakalala, M. C. 2023. *Forensic Intelligence: The Effectiveness of the Biometric-based Solution to Combat Mobile Fraud (July 18, 2023)*. *OIDA International Journal of Sustainable Development*, Vol. 16, No. 05, pp. 19-30.
- Mark M. L. and Lisa T. B. 2014. *Research Methods in Crime, Justice, and Social Problems*. 2<sup>th</sup> Edition. Oxford University Press
- Maxfield, M. G. & Babbie, E. 2015. *Research Methods for Criminal Justice and Criminology*. Belmont: Wadsworth.
- Maxfield, M. G. & Babbie, E. R. 2021. *Research Methods for Criminal Justice and Criminology*. Belmont, CA, Wadsworth Pub.
- Michael-Kramer, W. 2018. *The most common biometrics technology linked to online financial fraud and crime related schemes and their primary red flags*. Available at <https://iacrc.org/procurement-fraud/the-most-common-procurement-fraud-schemes-and-their-primary-red-flags/> (Accessed 14 March 2024).
- Mironov, M. and Zhuravskaya, E. (2016), "Biometrics technology linked to online financial fraud and crime related in procurement and the political cycle in tunneling: Evidence from financial transactions data", *American Economic Journal: Economic Policy*, Vol. 8 No. 2, pp. 287–321.
- 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.
- Mohajan, H. (2018), "Qualitative research methodology in social sciences and related subjects", *Journal of Economic Development, Environment and People*, Vol. 7 No. 1, pp. 23-48.
- Mohamed, Z. 2017. *Biometrics technology linked to online financial fraud and crime related. The key to understanding and mitigating biometrics technology linked to online financial fraud and crime related risks*. Available at: <http://www.procurementfraud.co.za/search/our-greedygovernment.php> (Accessed on: 7 November 2018).
- Morrow, S. L. 2015. *Quality and Trustworthiness in Qualitative Research in Counselling Psychology*. *Journal of Counseling Psychology*.



- Murray, J. 2014. The causes, impact and prevention of employee fraud. *Journal of Financial Crime*, 23(4): 1012-1027.
- Murray, J.G. (2024), "Biometrics technology linked to online financial fraud and crime related: A Case Paper", EDPACS, Taylor & Francis, Vol. 49 No. 5, pp. 7–17.
- Orthmann, C.H. & Hess, K.M. 2013. *Criminal Investigation*. 10th edition. Delmar: Cengage Learning.
- Osterburg, J.W. & Ward, R.H. 2010. *Criminal Investigation. A Method for Reconstructing the Past*. 6th edition. Boston: Anderson.
- PwC (2021), "Global economic crime survey", pp. 1-60, [Online], available at: [www.pwc.org](http://www.pwc.org) (Accessed on 3 January 2024).
- PwC. (2014), "Global Biometrics technology linked to online financial fraud and crime related Survey 2014", available at: <http://www.pwc.com/biometrics-technology-linked-to-online-financial-fraud-and-crime-relatedsurvey> (accessed 21 March 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](http://www.corruptionwatch.org.za/wp-content/uploads/2020/06/global-economic-crime-survey-20201.pdf) (Accessed on 17 January 2024).
- SABI for Economic Co-Operation and Development. (2016), Preventing Biometrics technology linked to online financial fraud and crime related in Public Procurement.
- Singleton, R.A. & Straits, B.C. 2010. *Approaches to Social Research*. New York: Oxford University.
- South African Banking Risk Information Centre (SABRIC) (2019), "Digital banking crime statistics", [Online], available at: [www.sabric.co.za](http://www.sabric.co.za) (Accessed on 2 February 2024).
- South African Banking Risk Information Centre (SABRIC) (2020), "Annual crime statistics", [Online], available at: [www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf](http://www.sabric.co.za/media/20oouwbg/sabric-annual-crime-stats-2020.pdf) (Accessed on 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](http://www.resbank.co.za/AboutUs/Functions/Pages/Management-of-the-South-African-money-and-banking-system.aspx) (Accessed on 2 February 2020).
- Taroni, F., Bozza, S., Biedermann, A., Garbolino, P. & Aitken, C. 2010. *Data analysis in forensic science. A Bayesian decision perspective*. West Sussex: John Wiley & Sons.
- Van Graan, J. & Budhram, T. 2015. Principles of Evidence. In Zinn, R.J. & Dintwe, S.I. (eds). 2015. *Forensic Investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta
- Van Niekerk, B. (2017), "An analysis of cyber-incidents in South Africa", *The African Journal of Information and Communication*, Vol. 20, pp. 113-132.
- Welman, J.C., Kruger, S.J. and Mitchell, B. 2010. *Research methodology for the business and administrative sciences*. (6<sup>th</sup> Edition). Johannesburg: Thomson.
- Zinn, R.J. & Dintwe, S.I. (eds). 2015. *Forensic investigation: Legislative Principles and Investigative Practice*. Cape Town: Juta.

