Lighthouse

The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy

ISSN 2957-8842 (Print)

Vol 1 Issues (1&2), 2022

©ZEGU Press 2022

Published by the Zimbabwe Ezekiel Guti University Press
Stand No. 1901 Barrassie Rd,
Off Shamva Road
P.O. Box 350
Bindura, Zimbabwe

All rights reserved

DISCLAIMER: The views and opinions expressed in this journal are those of the authors and do not necessarily reflect the official position of funding partners"

Typeset by Divine Graphics
Printed by ZEGU Press

EDITOR-IN-CHIEF

- Dr Ellen Sithole, Zimbabwe Ezekiel Guti University, Zimbabwe

MANAGING EDITOR

- Dr Noah Maringe, Zimbabwe Ezekiel Guti University, Zimbabwe

EDITORIAL ADVISORY BOARD

- Dr Sithabile Manyevere, University of Zimbabwe, Zimbabwe
- Dr Tinotenda Chidawu, University of Zimbabwe, Zimbabwe
- Dr Prolific Mataruse, University of Zimbabwe, Zimbabwe
- Dr Carren Pindiri, University of Zimbabwe, Zimbabwe
- Dr Kiriana Magaya-Dube, Great Zimbabwe University, Zimbabwe

SUBSCRIPTION AND RATES
Zimbabwe Ezekiel Guti University Press Office
Stand No. 1901 Barrassie Rd,
Off Shamva Road
P.O. Box 350
Bindura, Zimbabwe
Telephone: ++263 8 677 006 136 | +263 779 279 912
E-mail: zegupress@admin.uz.ac.zw

http://www.zegu.ac.zw/press

About the Journal

JOURNAL PURPOSE
The purpose of the *Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy is* to provide a forum for urban solutions based on a systems approach and thinking as the bedrock of intervention.

CONTRIBUTION AND READERSHIP
Lawyers, criminologists, economists, public policy experts, bureaucrats, students, researchers and many other experts located in both the private and public spheres.

JOURNAL SPECIFICATIONS
Lighthouse: The Zimbabwe Ezekiel Guti University Journal of Law, Economics and Public Policy

ISSN 2957-884 2(Print)

SCOPE AND FOCUS
The journal is a forum for the discussion of ideas, scholarly opinions and case studies on law and policy, statutes, constitutions, general rules of the game (institutional mechanisms) and policy pronouncements or declared positions that are put to scrutiny, weighed, interpreted and evaluated. In all these matters, the intention and context usually define the outcomes and impact. The journal is produced bi-annually.

Source from a Journal

Anim, D.O and Ofori-Asenso, R (2020). Water Scarcity and COVID-19 in Sub-Saharan Africa. *The Journal of Infection*, *81*(2), 108-09.
Banana, E, Chitekwe-Biti, B and Walnycki, A (2015). Co-Producing Inclusive City-Wide Sanitation Strategies: Lessons from Chinhoyi, Zimbabwe. *Environment and Urbanisation*, *27*(1), 35-54.
Neal, M.J. (2020). COVID-19 and Water Resources Management: Reframing Our Priorities as a Water Sector. *Water International*, *45*(5), 435-440.

Source from an Online Link
Armitage, N, Fisher-Jeffes L, Carden K, Winter K. (2014). Water Research Commission: Water-sensitive Urban Design (WSUD) for South Africa: Framework and Guidelines. Available online: https://www.greencape.co.za/assets/Water-Sector-Desk-Content/WRC-Water-sensitive-urban-design-WSUD-for-South-Africa-framework-and-guidelines-2014.pdf. Accessed on 23 July 2020.

Source from a Published Book
Max-Neef, M. (1991). Human Scale Development: Concepts, Applications and Further Reflections, London: Apex Press.

Source from a Government Department (Reports or Plans)
National Water Commission (2004). Intergovernmental Agreement on a National Water Initiative. Commonwealth of Australia and the Governments of New South Wales, Victoria, Queensland, South Australia, the Australian Capital Territory and the Northern Territory. Available online: https://www.pc.gov.au/inquiries/completed/water-reform/national-water-initiative-agreement-2004.pdf. Accessed on 27 June 2020.

The source being an online Newspaper article
The Herald (2020). Harare City Could Have Used Lockdown to Clean Mbare Market. *The Herald*, 14 April 2020. Available online: https://www.herald.co.zw/harare-city-could-have-used-lockdown-to-clean-mbare-market/. Accessed on 24 June 2020.

The Role of Technology in Evidence Gathering for Cases of Fraud: Case of Bulawayo Central Business District, Zimbabwe

DZINGAI KUDANGA[1], ADMIRE MTHOMBENI[2], EDWARD CHINONGWA[3], MATILDA SINGENDE, EDWARD TSHUMA[4] AND EVANS BONJISI TEMBO[5]

Abstract

This article discusses the role of technology in evidence gathering for cases of fraud, drawing reference from the Bulawayo Central Business District (CBD) in Zimbabwe. The research was inspired by the continued and endless occurrence of a plethora of scandalous fraud cases in the Bulawayo CBD. A mixed-method approach was adopted with a pragmatic philosophy. The approach gave inductive and deductive reasoning to conclude the relationship between technology and fraud. In this view, an exploratory design was used. The target population was mainly police officers and magistrates in the Bulawayo CBD. A questionnaire was used as an instrument to gather data, whilst Statistical Package for the Social Sciences (SPSS) was used for data analysis. Research results revealed that there is a positive relationship between the use of technology and the detection and prevention of fraud cases in the Bulawayo CBD. It was also established that fraudulent activities in the Bulawayo CBD encompassed both direct and indirect forms and the most prevalent fraud activities emanated from e-banking and were committed mostly by employees. The study recommends that there a need to continually train law enforcement agents, judicial officials and company staff on the use of technological tools and ways of detecting the current *modus operandi* of criminals about fraud-related activities.

Keywords: cyber laboratory, cyberspace, Information and Communication Technology

[1] Department of Business Studies, Police Staff College, Zimbabwe
[2] Business Management Department, Manicaland State University of Applied Sciences, Zimbabwe email-mthoadmire@gmail.com
[3] Human Resource Department, Midlands State University, Zimbabwe
[4] Administration Department, Police Staff College, Zimbabwe
[5] Department of Business Studies, Police Staff College, Zimbabwe

INTRODUCTION

The level of police performance across the globe is determined and measured mostly by the kind of satisfactory services accepted by members of the public being policed. On one hand, if the police perform very well, credit is given to the government and on the other hand, poor police performance puts the image of the police force into disrepute. It is irrebuttable that 21st century policing is coupled with new challenges emanating from technological advancement. In as much as criminals are taking advantage of technology and cyberspace, police organisations can also do better by technologically outpacing them. Therefore, this article seeks to unearth the role of technology in evidence gathering for cases of fraud drawing reference from the Bulawayo Central Business District in Zimbabwe. In a nutshell, fraud cases in the whole world have become a structural entity with an inherent conflict in the security sector and economic patterns (Albrecht, 1984; Dzomira, 2014; Davis, 2017). The detection, conviction and recovery of property from fraud cases remain worrisome and this calls for the use of technology as an aid to evidence gathering to secure a conviction.

For many years, the accounting field has been studying fraud; its genesis, *modus operandi*, consequences and various aspects (Dzomira, 2014). Albrecht (2005), as cited in Kapesa (2014), avers that fraud is rarely seen but its symptoms are usually observed. This, therefore, follows that great caution is needed whenever a fraud case is reported since in a court of law, the offence of fraud is not easy to prove beyond a reasonable doubt. For that reason, the discovery of fraudulent activities has made business entities embrace internal control systems, structured and designed in the best system of fraud management linked to sound corporate governance. At the global level, the embracement of technology to curb fraud led to the enactment of various policy frameworks and legislative measures. For example, the United States of America (USA) enacted the Sarbanes-Oxley Act — a control concept that prevents the repetition of scandals across the world as experienced by Enron. In Canada, the Canadian Institute of Charted Accountants enacted a policy framework for control of Information Technology (IT) in liaison with the Internal Control Worldwide Models (ICWM), as a way to prevent the spread of fraudulent activities.

In Nigeria, an Identity and Access Management (IAM) system was created to help reduce rampant fraud in the country. The system is commonly known as *Youverify* — aimed at streamlining how banks and other companies verify the identity of their customers, thereby exercising due diligence that tallies with know-your-customer (KYC) regulations (Oghojafor *et al.,* 2010). Along the same line of thinking, South Africa is on record for using digital forensic investigations and accounting knowledge on cyber fraud investigations and detection of fraud-related cases.

At the local level, Mawanza (2014) affirms that the adoption of the multi-currency system in Zimbabwe gave rise to cases of fraud. Musarurwa (2012), in Mawanza (2014), cited a KPMG report that indicated that the value of fraud in Zimbabwe in the six months to December 2011 soared to $1,2 billion, 32% of the overall value of fraud cases in Africa in the review period at $3,7 billion. He ranked Zimbabwe second to Nigeria, where fraud caused a loss of money over $1.6 billion, while South Africa recorded fraud above 35%, from 37% for a period extending from January to June 2011. In that vein, Dube *et al. (*2009) highlight that in Zimbabwe, electronic innovation began with the Standard Chartered Bank and the Central African Building Society (CABS) in the early 1990s when they installed automated teller machines (AT.). This led to volumes of interest in transactions as more people started to launch their monies in cyberspace and this allowed tech-savvy frauds (Dzomira 2014).

Furthermore, Zimbabwe has three different statute laws promulgated to curb the unwanted behaviour practised in cyberspace, namely the Postal and Telecommunications Act [Chapter 12:05], Censorship and Entertainments Controls Act [Chapter 10:04] and Criminal Law (Codification and Reform) Act [Chapter 9:23]. In Section 136 of the Criminal Law Codification and Reform Act, [Chapter 9:23] fraud includes cases committed through technological gadgets and manuals. It is against this background that the demand for accountability and acceptability by the general citizens in Zimbabwe drove the Zimbabwe Republic Police (ZRP) to formulate information system and technology strategies targeting cases of fraud for the value of money. Thus, the advent of the Information Technology and Fraud Management Strategy in the ZRP intends to meet the demands of a computerised society and at the same time streamlining the efficiency and effectiveness of police in dealing with fraud.

Currently, there are two cyber laboratory police stations in Zimbabwe — one situated in Harare Province and the other one in Bulawayo Province. Their main task is to conduct post-mortem forensic investigations using digital gadgets.

According to ZRP Khumalo Crime Register, Bulawayo Central District dealt with 488 fraud cases in 2019, of which 49 cases were cleared. In the year 2020, there was a total of 305 fraud cases. A fair percentage of the detected cases was aided by information supplied by network service providers such as Econet Wireless Zimbabwe and NetOne, among others. Nonetheless, several companies in Zimbabwe and across the globe lost billions of dollars due to fraudulent activities as indicated in Table 1.

Table 1: Statistics of Fraudulent Cases in Parastatals and Private Companies *(Annual Corruption Report, 2013-2021 and World History Fraud Cases, 2020)*

Year	Parastatals	Amount ($)
2001	Enron (USA)	US$74 billion
2002	World Communication USA	US$74 billion
2007	L&G Bedding Company (Japan)	US$1.4 billion
2012	Olympus Corporation (Japan)	US$1.5 billion
2013	Zimbabwe Broadcasting Corporation (ZBC)	US$900 000
2014	ZINARA	US$2015 650
	ZESA Holdings	US$6 million
	ZBC	US$1.3 million
	ZIMRA	US$1 million
	CMED	US$3 million
2015	Air Zimbabwe	US$10 million
	Central Vehicle Registry	US$16.5 million
2016	ZPC	US$5 million
	ZESA	US$500 million
2020	POSB	US$158 million
2020	Ministry of Health (Covid 19 graft)	US$60 million
2021	TM Pick &Pay	US$22 million

STATEMENT OF THE PROBLEM

Despite the emergence of technological management in fraud, there is no tangible improvement that curb escalation of fraud cases at in the Bulawayo CBD in Zimbabwe. As such, the detection, conviction and recovery of property from fraud cases by the ZRP remain worrisome, as the Bulawayo CBD has been experiencing a high

number of fraud-related cases. This is exhibited by several reported cases of fraud at police stations in Bulawayo as well as convictions secured in courts. More so, both social media and local newspapers are always swamped with reports of a fraudulent nature. This article seeks to determine the role of technology in evidence gathering in fraud cases, to increase the detection rate of the cases and eventual conviction in courts.

CONCEPTUAL FRAMEWORK

The conceptual model underlining this research combines a fraud Triangle that describes the behaviour of technology adoption and computer deception. The model intends to explore how deception and trust are exploited as antecedents of fraudulent behaviours (Cohen, 2013). The model describes how technological capabilities influence deception when opportunity, pressure and rationalisation create doors to deceitful exchanges (Albrecht *et al.*, 2012).

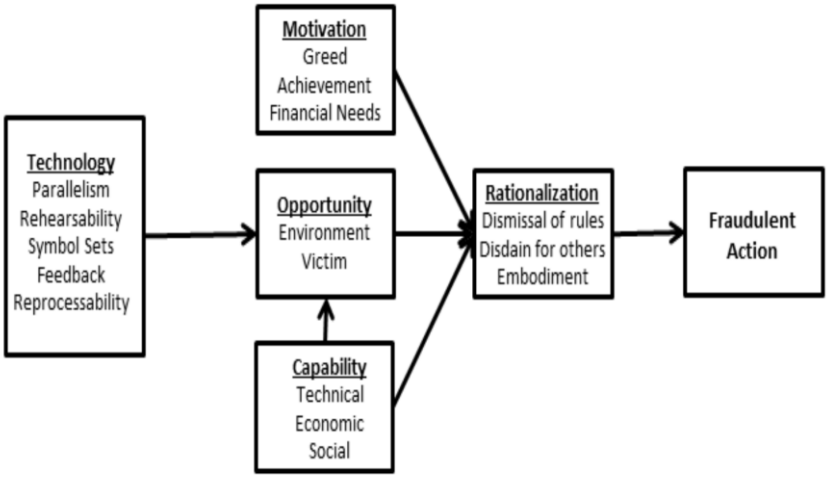


Figure 1: Conceptual Framework, Harrison (2014)

As depicted on Figure 1, Harrison (2014) avers that opportunity and ability do not directly cause behaviour but motivation (pressure) directly causes behaviour, whereas the relationship between motivation/pressure and rationalisation is moderated by ability and opportunity. The model, therefore, explains how technological tools create an electronic marketplace, the potential perpetrator's

technical, social and economic skills and ability to sense an opportunity to gain an advantage over others (Harrison *et al.,* 2017).

THEORETICAL FRAMEWORK

The theoretical framework of fraud-related activities is hinged on the Fraud Triangle Theory.

FRAUD TRIANGLE THEORY

This theory was propounded by Cressey as early as 1950 and it was originally deduced from Sunderland (1958)'s research on white-collar crimes. Cressey (1950), being a student of Sunderland, pursued the research basing the study on the factors that lead individuals to engage in fraudulent and unethical activities. The theory consisted of three elements: perceived pressure, opportunity and rationalisation.

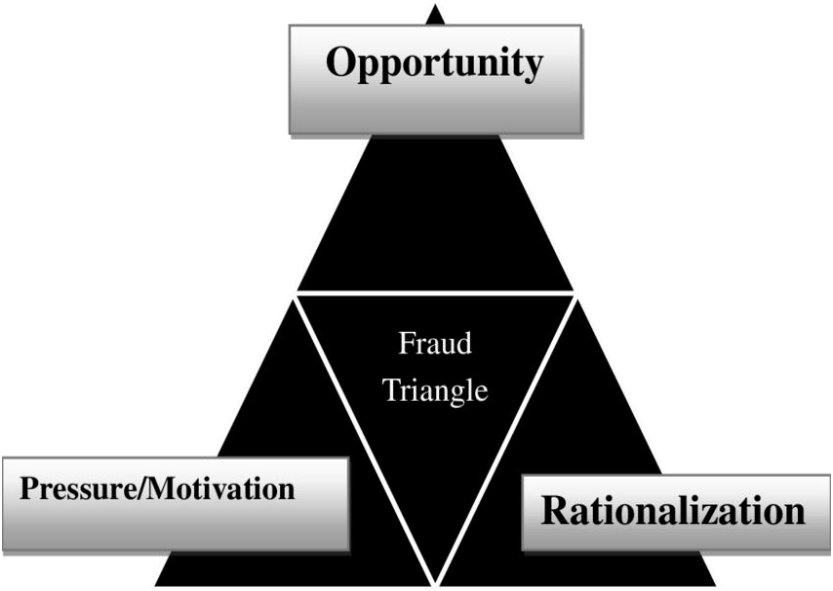


Figure 2: Fraud Triangle Theory *(Adapted from Cressey, 1971)*

Proponents of this theory perceived *pressure* as factors from unethical behaviour connected to McClelland's (1961) three motives that state that every individual's motive is to have power, self-actualisation and economic growth (Fatehi and Choi, 2019). As such, Abdullahi and Mansar (2015) conclude that financial or non-financial pressure cause individuals to commit unethical behaviour. The

theorists also provide that an *opportunity* to commit fraud is spearheaded by an ineffective control system or poor corporate governance system that allows an individual to commit fraud and, as such, individuals take advantage of the weaknesses of the internal control system. Along the same line of thinking, Cressey (1953) echoes that the lower the risk of being caught, the higher the likelihood of fraud taking place. *Opportunity* is considered an inherent condition that leads to an occurrence of fraud when there is an inadequate job division, weak internal control and irregular auditing (SPAM SOAP). Moreover, *rationalisation* is the justification and excuse where an individual's immortal conduct happens to be differentiated from criminal activities since an individual believes that he or she has the authority and right to claim ownership during the fraudulent behaviour.

THE MAIN TYPES OF FRAUD

Electronic fraud is classified into two broad categories, namely, direct and indirect fraud (Dzomira, 2014).

DIRECT FRAUD

Scientifically, direct fraud includes the use of credit or debit cards, embezzlement of money by employees and salami attacks. This is the unlawful usage of a credit or debit card by falsifying and obtaining of money or belongings without the knowledge of the card or debit card owner (Soleh, 2013). It involves impersonation and theft of identity, that is name and social insurance number (SIN) or personal identification number (PIN) (Ikechi and Okay, 2013).

EXECUTIVE MANAGEMENT'S FRAUD

Executive management fraud is committed by a trusted employee delegated to positions of authority. Management commits fraud by balance sheet restructuring and **w**indow dressing of organisational accounts. Executive fraud is in the form of collusion, own consumption by an employee, lending money to their cronies and non-refundable organisational funds (Hill and Jones, 2013). The unauthorised use of company or organisation assets by the executive is regarded as fraud. Usually, the money or property stolen by the executive is disposed of through money laundering and externalisation. Money laundering is a process of converting illegally obtained cash into untraceable transactions. The stolen cash appears legal after being reinvested into other businesses. In Bulawayo, both

private and public companies are being defrauded by management of the companies.

CREDIT FRAUD OR RISK ASSET MANIPULATION

Banks and money-lending companies in Bulawayo are financial intermediaries facilitating credits to individuals and the government. Individuals borrow money from intermediaries to start or expand their businesses while the government borrows money to reboot its fiscal policies meant to improve the welfare of its people. Loans are the typical type of credit granted by banks and other financial institutions. Financial managers both in the private and public sectors facilitate fraudulent activities by accepting prescribed forms that do not have full particulars of the credit applicant. Fictitious bank accounts are created with untraceable records and, therefore the funds are never recovered. To curb fraud both in theese sectors, the government of Zimbabwe promulgated the Public Procurement and Disposal of Public Assets Act [*Chapter 22:23*].

ADVANCE FEE FRAUD

Advance fee fraud is a scam where fraudsters approach and misrepresent to an individual, company or bank, very lucrative or favourable business terms. They sometimes offer access to large pools of funds at below-the-market interest rates. Theese fraudsters will convince the potential victim to pay a certain amount as an advance fee or processing fee. Once the money is paid, the perpetrators stop further communication with the victim and disappear. In Bulawayo, criminals have been hacking EcoCash and WhatsApp accounts using stolen identities of persons trusted by others in a WhatsApp group, offering United States dollars or South African rands at good rates of exchange. After receiving the local currency through Eco-Cash, they vanish. Complainants throughout the country lost around US$100 million in 2021 through this method. ZRP Police spokesperson, Assistant Commissioner Paul Nyathi once commented that Bulawayo a pensioner lost $29 000 of his pension payout to con-artists who promised to sell him US dollars once they received his money through Eco-Cash (*The Herald,* 13 April, 2021).

Criminals in Bulawayo were also getting access to banks systems and then they call the victim pretending to be a bank employee requesting him/her to supply his/her details on the pretence that the bank was updating the information in their system. After getting the

victim's details, he criminals then transfer the money from the person's bank account into the criminals' Eco-Cash or bank accounts. They quickly withdraw the money from the bank or cash it out at Eco-Cash pay-out points where they cannot be tracked (*The Herald,* 13 April 2021).

Furthermore, many people in the Bulawayo CBD are duped by criminals who advertise jobs or services in the media or on WhatsApp platforms that they usually join through group links. The unsuspecting victims will be asked to send a registration fee through Eco-Cash to get a tender or a job and soon after the money has been sent, the criminals will no longer be reachable.

Moreover, some employees in the Bulawayo CBD and at their various working places are taking advantage of weak control systems. According to the Nations on Occupational Fraud and Abuse 2014 Report, organisations lose 5% of their revenues to fraud each year. Bernie Brown (2014), CFO of Coppermine Bakery Holdings, posited that there were three major categories of occupational fraud: asset misappropriation only, corruption along with asset misappropriation and financial statement fraud. These three categories of fraud damage business finance and reputation.

COUNTERFEIT SECURITIES FRAUD

In this case, the fraudster uses counterfeit financial documents. The advent of modern photographic and printing equipment has made it easy for fraudsters to obtain complete counterfeits or entirely forged documents through technology to alter amounts, dates, names and other important document features. This includes the printing of fake money, fake driver's licences, fake birth certificates or fake agreements of sale. This has resulted in serious losses of both corporeal and non-corporeal property in the Bulawayo CBD in Zimbabwe.

ACCOUNT OPENING FRAUD

The fraudster uses fictitious documents to open a bank or credit account. The fraudster can utilise these accounts to dupe the lender or the creditor. The fraudulent activity is so perfect that the whole process seems to be authentic and escapes any suspicion.

INSURANCE FRAUD

This surmounts false claims or exaggeration of an insurance premium that leads to loss to the insurer as the claim does not suffice the purpose of the insurance.

INDIRECT FRAUD

McGuire and Dowling (2013) describe indirect fraud as phishing, pharming, hacking, virus spam and malware. These elements facilitate fraud by either deleting, formatting or changing the contents of the information with the intention to mislead. Indirect fraud falls into any of the following sub-categories.

COMPUTER FRAUD

Computer fraud is more sophisticated than the manual one as it involves technological gadgets. This kind of fraud is accomplished by tampering with computer programs, data files, operations, equipment or media. Some criminals in Bulawayo hack company databases and defraud the companies and/or their clients. These fraudsters also hack the victim's Eco-Cash and WhatsApp accounts, leaving the victims' phones without network connectivity. The cybercriminals then pose as friends in the WhatsApp groups the victims belong to, offering United States dollars at lucrative rates. Some members of the group may then transfer money by Eco-Cash to their friend's accounts without any suspicion. When the fraudsters, who now control the victims' accounts receive the money, they vanish.

ELECTRONIC BANKING FRAUD

The advent of e-banking has resulted in the development of new financial products and various business transactions in the world. E-commerce has spawned a wide range of fraud activities perpetrated by the internet. The internet, through electronic cards, makes it possible for fraudsters to access the details of account holders and stake their finances without them knowing. Credit cards involves cloning whereby the criminal copies the stolen card information from an electronic device and swindles the cardholder (Singh and Jain, 2020).

THE ROLE OF TECHNOLOGY IN EVIDENCE GATHERING ON FRAUD-RELATED CASES

According to Boyle and Vullierme (2013), technology in cybercrime assists investigators to conduct covert surveillance. For example, the

Police Service of Scotland (2018) designed digital devices on mobile devices and internet-enabled objects that investigate cybercrimes in a manner that guides the admissibility of collected evidence in a court of law, whereas, in India, the Data Security Council of India (2011) had concluded some critical processes to be followed during the investigation of cybercrimes.In Zimbabwe, the Police Criminal Investigations Cyber Laboratory Department has the technological tools monitor cyberspace and gather evidence to secure a conviction. The crime scene not onlythe physical location of the digital device used in the commission of cybercrime. If the devices are available, the police document the scene before collecting the evidence. The documentation covers how the digital devices have been used in the collection of evidence and their operating state, physical characteristics, make, model, serial number or markings (Steuart, 2015).

Maras (2014) reiterates that logical extraction plays imperative vitally important role in seeking evidence from the location of the digital devices. This evidence is relevant for filing found in computer operating systems to facilitate keeping track of records, names, location of files and storage. Generally, in the accounting system, there are external controls, internal controls and codes of ethics. These three controls attempt to control and prevent fraud and errors by roping in regulations. In a way, technology regulates corporate accountability by promoting auditor independence and the implementation procedure of rotating auditors after five years to prevent them from offering non-audit services (Dattin, 2017). Technology strengthens the independence of audit committees and requires CEOs or CFOs to verify and certify financial statements (*ibid.*).

In terms of law, the Sarbanes-Oxley Act of the USA advocates that technology should state auditing standards, a provision that points out the position of external control where fraud is involved. As such, a business that uses the Enterprise Resource Planning (ERP) system makes it easy for judicial proceedings to assess the rules and guidelines on how the business manages risk in preventive, detective and corrective cases.

Research by Golden *et al*. (2014) reveal that technology provides detective ways that prove the effective use of anonymous hotlines or

tip lines. Further research by King (2016) shows that employees use other fraud reporting methods like anonymity and confidentiality. In a way, the involvement of tip lines increases management's knowledge and detection of ethical misbehaving, complaints and potential fraud occurrences. Generally, worldwide, it was proven that through technology, police are now using emails, social media platforms like Facebook, WhatsApp, among others, to detect fraud (Sunde, 2017; Rempel, 2019).

Bonnet *et al*. (2019) in their social science research suggest that presiding officers construct a story from the evidence and retain evidence that is consistent with the story. Macue (2016) supports Bonnet (2019) when he says justice is an exhibition of showmanship that provides the jury with information both in form and content and assists them in reaching a rational and fair conclusion. Animation makes the computer generate admissibility with its ability to re-construct the scene. Animations assist the jury by making a thorough analysis of accuracy, relevance and avoidance of unfair prejudice (Shelton *et al.,* 2016). Animations rebut the defence of rationalisation. The simulation takes on from where animation fails by linking the sequences of events and synthesising information based on inadmissibility. The scientific evidence tests the part played by the simulation to assess the validity of methods involved in evidence gathering. The National Prosecuting Authority (NPA) of Zimbabwe requires simulation to be scrutinised to avoid the admission of unreliable evidence through computer programs to guard against human and programming errors in the underlying software (National Prosecuting Authority, 2018).

EMPIRICAL REVIEW

Lee (2021) conducted research on online fraud victimisation in China in 2021 based on online shopping webs. In the study, the data analyzed were collected and derived from publicly accessible web fora based in China. The web forum, Baidu Tieba, on which information, goods and services are exchanged, was started in 2003. The study used multiple correspondence analysis (MCA) and chi-square tests to understand patterns of online fraud in China's Baidu Tieba. The research used MCA to understand online fraud victimisation and, in particular, explore what types of media, methods and resources were used to commit such crimes as well as identify types of victimisation they intersect with. The study

observed trends in China's online fraud victimisation in the current data. The number of cases grew rapidly and a total of 129 cases, or 49% of the whole dataset, were reported in 2017. Fewer than 10% of the cases were reported from 2008 to 2012. With further penetration of technology and the use of Baidu Tieba as a platform, more than 90% of cases were documented from 2013 to 2017. The research found out that there are two types of online fraud showing particularly interesting results: Refund fraud (an online non-delivery fraud) is one type of crime in which customer payments are made without the delivery of goods and services. Return fraud (an online non-payment fraud), on the other hand, is a type of fraud in which goods and services are delivered without payment being made and then fraudulently requesting money. Only one type of fraud was linked to the online payment system Alipay, that is refund fraud (100.00%), while phones were used to commit four different types of fraud; proportionally speaking, the most common were return fraud (61.54%), followed by fake contact (19.22%), card fraud (9.63%) and phone bill fraud (9.61%). Phones were not used in refund fraud victimisation. To carry out refund frauds, fraudsters typically advertise an item, product, or service on a classified-advertisement website and contact potential targets via e-mail or phone.

Ngalyuka (2013) carried out a study to establish the relationship between ICT utilisation and fraud losses in commercial banks in Kenya. Secondary data was used to collect statistical data from existing records at the Banking Fraud Investigation Unit (BFIU). CBK reports gave data collected from transactions done through ATM, RTGS and EFT. The data on staff costs were extracted from audited financial statements of banks for the period 2008-2012. The collected data were analyzed using the Statistical Package for Social Sciences (SPSS) version 16. Regression analysis was used to quantify the relationship between the dependent variable and the independent variables. The analysis of data was for 43 registered commercial banks. The researcher concluded that commercial banks recorded an increment in ICT utilisation and fraud costs. The minimum and maximum fraud losses were ksh68.49 million and ksh124.17 million, respectively. The mean EFT, RTGS and ATM values were shs4,334 million, shs262,300 million, shs1,501,146 million and shs9,595 millio,n respectively for the study period. The minimum and maximum ATM values were ksh5276.64 million and ksh15, 022 million, respectively. The main conclusions of the study indicated

that ICT utilisation exposes commercial banks in Kenya to more fraudulent activities. The adoption of ICT identifies thefts of money transacted online. The level of staff wages also had a positive correlation with fraud losses. Ngalyuka (2013) recommended more robust fraud mitigation practices and policies to ensure that all elements of fraud are captured in the adoption of ICT. Ngalyuka (*ibid.*) concluded that bank employees have access to all information relating to customer accounts, hence they should be well rewarded and motivated to prevent them from falling into traps of fraud.

Chigada (2020) investigated end-users' perceptions about the feasibility of installing biometric authentication systems as interventions to ameliorate card fraud in the South African payment card industry. The research concluded that banks were not keen to invest in an outright biometric environment because of the huge costs that would be incurred in implementing advanced technologies. The cost entails hiring SAP consultants and IT professionals and acquiring software and hardware (Focus Group, 2019).

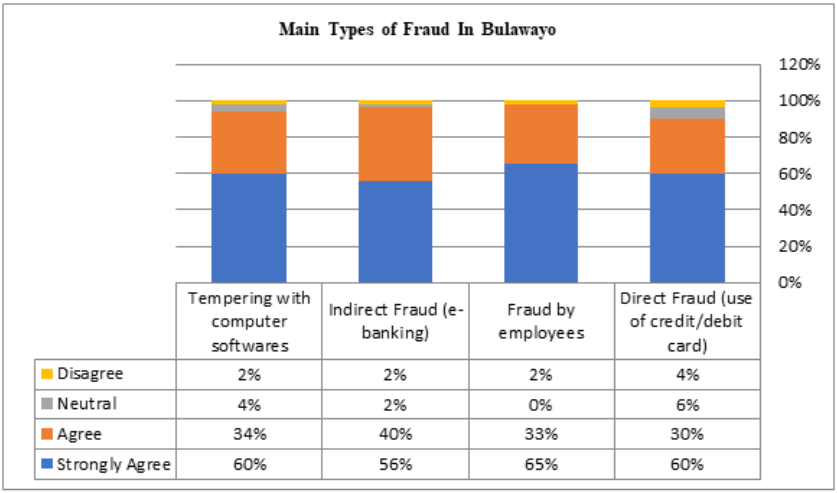
The objective of the study was to determine if the existing banking technology and telecommunications infrastructure could support biometric payment systems to determine the detection and apprehension of a fraudster during bank account management systems. Concerning Chigada's study (2020), it is the objective of every government to provide a code of governance that fosters a good culture of corporate governance in observance and adherence to regional and best practice in international governance to curb fraud activities. Chigada (*ibid.*) concluded that the implementation of biometric systems required highly skilled information technology personnel to oversee and support these technologies. This was identified as a potential hindrance for banks. The study established that existing banking and telecommunications infrastructure was capable and supported biometric systems. The findings also showed that the introduction of zero-floor limits led to high traffic volumes, creating congestion in telecommunications connectivity. Chigada's (*ibid.*) in coherence with King George III's code of corporate governance, has established that banking technology and telecommunications infrastructure were capable of supporting biometric payment systems. He also concurred with the objectives of the corporate governance framework where its mandate is to clarify relationships, reporting structures, transparency and role clarity in

responsibility and accountability and controlling risks. His study revealed that the deployment of biometric systems would mitigate card fraud transactions.

RESEARCH METHODOLOGY

The researchers adopted a mixed-method approach with a pragmatic philosophy. The approach gave inductive and deductive reasoning to conclude the relationship between technology and fraud. In this view, an exploratory design was used. The target population was mainly police officers and magistrates in the Bulawayo CBD. The sample size was 120 respondents that were arrived at using the Krejicie and Morgan 1970 Determination Scale. Questionnaires were used to gather data.

RESULTS



	Tempering with computer softwares	Indirect Fraud (e-banking)	Fraud by employees	Direct Fraud (use of credit/debit card)
Disagree	2%	2%	2%	4%
Neutral	4%	2%	0%	6%
Agree	34%	40%	33%	30%
Strongly Agree	60%	56%	65%	60%

Figure 3: The Main Types of Fraud in Bulawayo Central District *(Researchers, 2022)*

The analysis in Figure 3 indicates that most types of fraud are committed by employees as 65% strongly agreed that most employees are involved in fraud cases. The results are supported theoretically by Cressey (1950) and Wolfe and Hermanson (2004) by alluding that opportunity to commit fraud is considered an inherent condition that leads to an occurrence of fraud by employees when there is an

inadequate job division, weak internal control and irregular auditing. The reason for most employees to be involved in fraud cases is believed to emanate from unethical behaviour that is connected to McClelland theory (Kurt, 2021; Hoffman, 2019). Along the same line of thinking, Sunderland (1939), Cressey (1950) and Wolfe and Hermanson (2004) argue that employees engage in fraudulent activities due to perceived pressure, rationalisation, opportunity and capacity. A total of 56% of respondents strongly agreed that e-banking fraud was also a common form of fraudulent activity being experienced in the Bulawayo CBD since it is where the majority of business transactions involving huge amounts of money takes place. In the same vein, 60% of the respondents strongly agreed that fraud involving the use of credit/debit cards was prevalent in the Bulawayo CBD. Finally, the majority of the respondents (60%) also considered tempering with computer software as another main type of fraudulent activity being experienced in the area under study. Therefore, it can be inferred that most of fraudulent activities occurring in the Bulawayo CBD are technology related and as such one cannot underscore the role of technology in evidence gathering for fraud-related cases.

THE ROLE OF TECHNOLOGY IN EVIDENCE GATHERING FOR FRAUD-RELATED CASES IN BULAWAYO CENTRAL BUSINESS DISTRICT IN ZIMBABWE

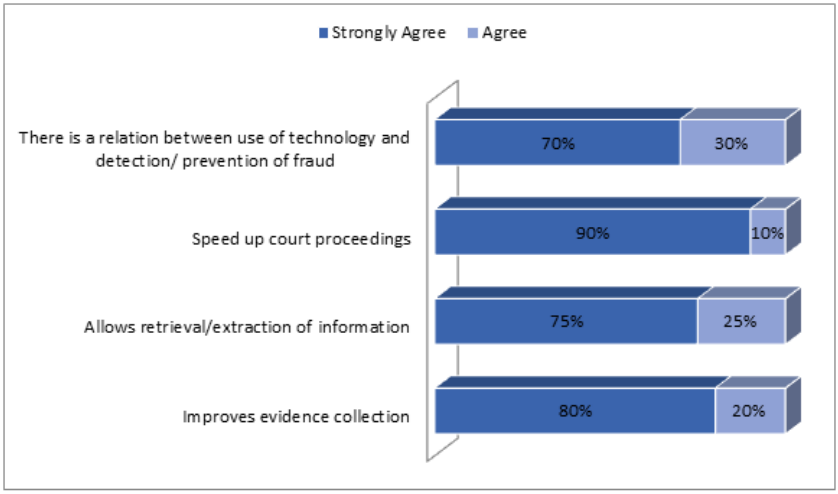


Figure 4: The Role of Technology in Evidence Gathering for Fraud-related Cases *(Researchers, 2022)*

Figure 4 indicates that 70% of the respondents strongly agreed and 30% agreed that there is a relation between the use of technology and the detection and prevention of fraud cases in the Bulawayo CBD. A total of 75% of the respondents strongly agreed that technology allows the retrieval and extraction of information used in the commission and omission of fraud cases in the Bulawayo CBD, whereas 25% unanimously agreed that technology is very essential in evidence gathering as it enables the extraction of information. A majority of respondents (90%) strongly agreed that technology speeds up court proceedings, while only 10% . A total of 80% of the respondents strongly agreed that technology improves methods of evidence collection from the location of the scene where evidence resides. Data collected from respondents concurred with the research conducted by Bonnet (2019), Marcus and Oransky (2017) and Stuart (2015) whose conclusions established that technology assists with documentation of how technology is used in data collection and its involvement in physical and logical extraction within the location of where evidence resides.

CONCLUSIONS AND RECOMMENDATIONS

From the study, it has been discovered that computer apparatus is admissible only if the tools can present a fair and accurate reflection of the oral testimony being offered by a person to the judicial officer. Computers help presiding officers to understand difficult concepts of interactive multimedia by presenting communication where the audience relies on visual information. The movement of information on technological tools leaves prints that can be traced and lead to the chain of evidence in court where the magistrate will use that evidence to convict or acquit accused persons. ICT tools are admissible in court if they can identify, collect, acquire and preserve evidence that is lost through volatility and fragility. Computers capture, store, image, process and retrieve information that attracts admissibility if such components bring credibility and reliability during the process of evidence gathering.

Police organisations should move with the changes in technology and equip all their stations with technological gadgetry to use to detect or prevent fraud cases through conducting post-mortem forensic investigations. There is also a need to continually train law enforcement agents, judicial officials and company staff on the use

of technological tools and ways of detecting the current *modus operandi* of criminals in fraud-related activities.

REFERENCES

Albrecht, W.S., Howe, K.R and Romney, dan M. B (1984). Deterring Fraud: The Internal Auditor's Perspective. Altomonte Springs, FL: The Institute of Internal Auditors' Research Foundation.

Albrecht, W.S., Albrecht, C and Albrecht, dan C.O (2006). *Fraud Examination*. New York, NY: Thomson South-Western. Association of Certified Fraud Examiners.

Bonnet, Y. (2021). Surrogacy in France: A Summary of the Situation. *Bioethica*, *7*(1), 64-70.

Chigada, J.M. (2020). A Qualitative Analysis of the Feasibility of Deploying Biometric Authentication Systems to Augment Security Protocols of Bank Card Transactions. *South African Journal of Information Management*, *22*(1), 1-9.

Cressey, D. R. (1950). The Criminal Violation of Financial Trust. *American Sociological Review, 15*(6), 738-743.

Cohen, J. (2013). Statistical *Power Analysis for the Behaviour Science. 2 Ed*. Hillsdale, NJ: Lawrence Erlbaum Associates, Publishers.

Dattin, C.F. (2017). Developments in France Regarding the Mandatory Rotation of Auditors: Do they Enhance Auditors' Independence? *Accounting History*, *22*(1), 44-66.

Davis, C. (2017). Police Leadership: An Exploratory Study of the Perceptions of Police Officers. United Kingdom: Nottingham Trent University.

Dzomira, S. (2014). Electronic Fraud (Cyber Fraud) Risk in the Banking Industry, Zimbabwe. *Risk Governance and Control: Financial Markets and Institutions*, *4*(2), .16-26.

Fatehi, K and Choi, J. (2019). *International Business Management: Succeeding in a Cultural Diverse World*. 2 Ed. Springer Texts in Business and Economics. 13(2)., 96–108

Golden, R.E and Warner, K. (2014). The Global Reach of Seafood Fraud: A Current Review of the Literature. *Oceana*, 9(2)., 1–11

Harrison, C., Burnard, K and Paul, S. (2017). Entrepreneurial Leadership in a Developing Economy: A Skill-based Analysis. *Journal of Small Business and Enterprise Development*, *25*(3), 521-548.

Kapesa, T. (2014). Forensic Auditing of Related Party Transactions in Zimbabwean Banks to Avert Fraud. Gweru: Midlands State University.

King, D. (2016). *Fiscal Tiers (Routledge Revivals): The Economics of Multi-Level Government*. WHERE PUBLISHED: Routledge.
Lee, P.W. (2021). *From Dead Ends to Cold Warriors: Constructing American Boyhood in Postwar Hollywood Films*. WHERE PUBLISHED: Rutgers University Press.
Maras, M.H. (2014). *The CRC Press Terrorism Reader*. WHERE PUBLISHED: CRC Press/Taylor & Francis Group.
Marcus, A and Oransky, I. (2017). Is There a Retraction Problem? And, If So, What Can We Do About It. In*The Oxford Handbook of the Science of Science Communication* (119-126). New York: Oxford University Press.
Mawanza, W. (2014). An Analysis of the Main Forces of Workplace Fraud in Zimbabwean Organisations: The Fraud Triangle Perspective. *International Journal of Management Sciences and Business Research*, *3*(2), 1-12.
McClelland, C.A. (1961). The Acute International Crisis. *World Politics*, *14*(1), 182-204.
Musarurwa, D. (2012). $1,2bn Fraud Cases in Six Months. *The Sunday Mail*, 12, May 2012. Available online: http://maravi.blogspot.com/2012/05/sunday-mail-zw-12bn-fraud-cases-in-six.html
Ngalyuka, C. (2013). The Relationship Between ICT Utilization and Fraud Losses in Commercial Banks in Kenya. Doctoral Dissertation, University of Nairobi.
Oghojafor, B.E.A., Olayemi, O.O., Okonji, P.S and Okolie, J.U. (2010). Poor Corporate Governance and its Consequences on the Nigerian Banking Sector. *Journal: Siberian Journal of Management*, *5*, 243-250.
Rempel, E and Burke, T. M. (2022). Technology on Trial: Facilitative and Prejudicial Effects Of Computer-Generated Animations On Jurors' Legal Judgments. *Psychology, Crime & Law*, 1-23.
Shelton, A.J., Wojciechowski, Ł.P and Warner, J. (2016). Ambient Marketing Practices in the United States: A Professional View. *Communication Today*, *7*(1), 18-29.
Singh, A and Jain, A. (2020). An Empirical Study of AML Approach for Credit Card Fraud Detection–financial Transactions. *International Journal of Computers Communications & Control*, *14*(6), 670-690.
Stuart, D. (2015). Under Scrutiny. *Company Director*, *31*(6), 54-57.

Sunde, T. (2017). Foreign Direct Investment, Exports and Economic Growth: ADRL and Causality Analysis for South Africa. *Research in International Business and Finance*, *41*, 434-444.

Sunderland, E.S. (1958). Suggestions for Improvement in Section 77 of the Bankruptcy Act. *Bus. Law.*, *14*, 487.

Sutherland, E. H. (1939). White-Collar Criminality. *American Sociological Review, 5* (1),1-12.

Wolfe, D. T and Hermanson dan D (2004). The Fraud Diamond: Considering the Four Elements of Fraud. *The CPA Journal*, *74*(12), 38.