The Effects of Cyber Fraud on Higher Education Financial Aid Students in South Africa

A Dissertation presented

to the Department of Information Systems

University of Cape Town

By

Gershon Hutchinson

(HTCGER001)

Supervisor: Associate Professor Salah Kabanda

In partial fulfilment of the requirements for the
Master of Commerce degree in Information Systems 2023

Declaration

1. I know that plagiarism is wrong. Plagiarism is to use another's work and pretend that it is one's own.
2. I have used the APA convention for citation and referencing. Each contribution to, and quotation in, this Research Proposal '*The effects of Cyber Fraud on Higher Education Financial Aid students in South Africa'* from the work(s) of other people, has been attributed and has been cited and referenced.
3. This paper is my own work.
4. I have not allowed, and will not allow anyone, to copy my work with the intention of passing it off as his or her own work.
5. I acknowledge that copying someone else's assignment, essay or paper, or part of it, is wrong, and declare that this is my own work.

Signature: G…J…….

Date: 03.04.2023

Full Name of Student: Gershon Hutchinson

ABSTRACT

Due to the exponential growth of the internet, cyber fraud has become an increasingly prevalent issue globally, and South Africa is no exception. Financial aid is critical to enabling higher education for many South African students, particularly those from disadvantaged backgrounds. The NSFAS has repeatedly cautioned students regarding fraudsters using a variety of techniques, including phishing, vishing, spoofed websites, and social media, which criminals employ to access their allowances. Yet, cyber-crime, particularly cyber fraud continues to infiltrate the higher education sector and many others in South Africa. Understanding the unique challenges faced by South African higher education financial aid students concerning cyber fraud is essential for developing preventive strategies and providing support. It is crucial to understand the effect of cyber fraud on these students, as cyber fraud can severely affect their educational opportunities and well-being. The goal of this study is to identify and understand how South African higher education financial aid students perceive cyber fraud; and how cyber fraud affects them.

The study employed a qualitative research design and utilized purposive and snowball sampling techniques to select participants. A semi-structured interview instrument, informed by existing academic literature, guided the conversation. Thirty active semi-structured interviews were conducted with students affected by cyber fraud to gain a comprehensive understanding of the topic. Inductive thematic analysis was employed for data analysis. Patterns in the data were identified, grouped to form overarching themes.

The findings show that all participants in this study experienced financial losses. The study found that 90% of participants had no formal or informal training on cyber fraud. The data suggests that most students lack the knowledge and skills to identify and protect themselves against fraudulent activities. Sixty-two percent of participants reported that the cyber fraud had a negative effect on their education, with 27% confirming that it affected their grades and 35% dropping out of school. The study found that some victims coped better than others, with those having financial or emotional support recovering more easily. The findings underscore the urgent need for training and awareness programs tailored explicitly for financial aid students, particularly those receiving financial aid for the first time. Beyond the immediate financial losses, the study also highlights the psychological, emotional, behavioural, and secondary affects experienced by affected students. It underscores the crucial role of support systems in determining students' academic success. Future research could explore the most effective methods for delivering training and awareness programs to financial aid recipients to protect them from cyber fraud.

Keywords: Cyber Fraud, Online Fraud, NSFAS, College students, financial aid, South Africa

ACKNOWLEDGEMENTS

The successful completion of this research project was made possible through the invaluable support and guidance of various individuals and organisations. I sincerely thank my academic supervisor, Associate Professor Salah Kabanda, for her help, expert advice, and constructive feedback throughout this research. Her mentorship played a crucial role in shaping the direction of this work. I would also like to thank the esteemed academics and dedicated support staff of the Faculty of Commerce at the University of Cape Town for their invaluable assistance and support, which have been instrumental in helping me reach this milestone.

I also wish to acknowledge Dr. Laban Bagui, who generously contributed his time and insights to this paper. His critical feedback and recommendations significantly enhanced the quality of this research project. Furthermore, my sincere thanks go to Raisibe Seroka for her exceptional efforts in conducting participant interviews and transcribing the transcripts. Her multilingual proficiency in various South African languages greatly facilitated the completion of this project. I want to thank the National Student Financial Aid Scheme (NSFAS) management for providing access to a list of potential research participants. Their support was instrumental in the completion of this project. I also want to thank the participants for taking the time to be part of this research project and sharing their experiences. Last, I want to acknowledge my daughter, Gabriella Hutchinson, for her patience, encouragement, and understanding throughout this challenging journey.

Table of Contents

List of Tables and Figures

List of Tables

List of Figures

List of Abbreviations

DHET - Department of Higher Education and Training

NSFAS - National Student Financial Aid Scheme

SABCF – Student Affected By Cyber Fraud

TVET - Technical and Vocational Education and Training

HEI - Higher Education Institution

CHAPTER ONE

1. INTRODUCTION AND BACKGROUND

1.1 Introduction

Due to the exponential growth of the internet, cyber fraud has become a significant problem worldwide, with no countries being immune to it (Ali & Mohd Zaharon, 2022). Fraud has existed since humans could talk and amass things (Button, 2017). There are various types of cyber fraud, including financial scams, phishing scams, contest or sweepstakes scams, technical support scams, and rogue security software (Hidayati et al., 2021). Examples of cyber fraud include advance fee fraud, where victims are made to believe that they can get huge returns for a small donation; lottery scams, where victims are solicited for a fee to release the winnings; and romance scams, where manipulated victims send money to a fake online identity (Whitty, 2019).

Technological advancements have made it easy for cybercriminals to reach millions of potential victims worldwide (Cross & Holt, 2021). This has turned cybercrime into a borderless crime, one of the significant challenges in combating it (Ajoy, 2022). Complicating matters further is the fact that as cyber fraud changes and adapts to its current environments, it has the potential to evade detection and prosecution (Vousinas, 2019). These challenges are even more dangerous in contexts that fail to enact cybersecurity practices and other security and privacy legislations. Africa has been identified as one of these contexts, which presents a fertile environment for cybercriminals due to its insufficient public understanding of cyberspace risks, inadequate development of digital infrastructure, low institutional capacity to coordinate and enforce existing cybersecurity laws, and a lack of comprehensive cybersecurity policies (Saeed & Osakwe, 2021). South Africa has been listed as a country with one of the world's highest instances of economic crime, with fraud as the most significant contributor (Mykhalchenko & Wiegratz, 2019).

While there have been several efforts to address the shortcomings that create a fertile environment for cybercriminals, limited studies exist that seek to understand the effect of cyber fraud on its victims (Button et al., 2014; Button, 2017; Button et al., 2021a; Knüpfer et al., 2021; Ochoa Hernandez et al., 2021). Understanding these effects is essential because the people affected by cyber fraud are often the ones in vulnerable positions (IPSFF, 2020). This study focuses on South African higher education financial aid students who are perceived to be vulnerable as they come from poor backgrounds. The National Student Financial Aid Scheme (NSFAS), the most significant provider of financial assistance in South Africa, defines

poor and working-class families as households with combined earnings of less than R350 000 per annum (Garrod & Wildschut, 2021). This study aims to understand the effect of cyber fraud on higher education financial aid students in South Africa.

1.2 Problem Statement

Cybercrime is a growing global threat, and insufficient awareness of cyber threats can have lasting and detrimental effects on the youth who lack knowledge of safe technology usage (Alqahtani, 2022; Aphane, 2023). Cyber fraud can lead to financial losses, identity theft, loss of trust in institutions, and self-blame, which can all affect the overall well-being of victims (Button & Cross, 2017). Notably, there is a lack of research on understanding the effect of cyber fraud on its victims, as noted by Button (2017), Button et al. (2014, 2021a), Knüpfer et al. (2021), and Ochoa Hernandez et al. (2021), especially amongst college students as emphasised by Alqahtani (2022). Aphane (2023) found that the youth lack the necessary vigilance to detect potential online threats due to a lack of awareness of internet risks.

Financial aid plays a crucial role in enabling higher education for South African students, especially those from disadvantaged backgrounds, as highlighted by Garrod and Wildschut (2021). MMapatji (2023) emphasises the significance of NSFAS allowances intended to support students with accommodation, transportation, and personal expenses, highlighting potential adverse consequences, such as inciting protests, declining academic performance, and even leading to dropouts. The NSFAS has repeatedly cautioned students regarding fraudsters using a variety of techniques, including phishing, vishing, spoofed websites, and social media, which criminals employ to access their allowances (Bhengu, 2021; NSFAS, 2021b; Samuels, 2021). Students receiving financial aid who have fallen victim to cyber fraud protested the NSFAS, alleging the unauthorised disappearance of their allowances from their accounts (Mbovane, 2019). Although several studies have examined how to ‘curb the prevalence of cybercrime perpetrated against students’ in South Africa (Mothibi & Amali,2018,57), the problem persists, despite most students being aware of the unethical cyber behaviours (Masenya 2023) and HEIs investment in expensive current security tools and changing strategies in countering latest cyber security attacks (Maranga & Nelson, 2019).

This study aims to investigate the effect of cyber fraud on South African higher education financial aid students, including their knowledge and awareness of cyber fraud risks, the types of cyber fraud they experience and the measures they take to protect themselves. Financial aid recipients are particularly susceptible to cyber fraud, given their reliance on financial services and potentially limited financial resources to mitigate losses. Understanding the

unique challenges faced by South African higher education financial aid students concerning cyber fraud is essential for developing preventive strategies and providing support. Overall, this study addresses a critical knowledge gap and contributes to understanding the challenges and experiences of South African higher education financial aid students in the context of cyber fraud. The study's findings can inform the development of effective prevention and response strategies to support these students and ensure they can access safe and secure educational opportunities.

1.3 Research Questions and Objectives

- What are South African higher education financial aid students' perceptions of cyber fraud?
- How are South African higher education financial aid students affected by cyber fraud?

Objectives of the study are:

- To understand how South African higher education financial aid students perceive cyber fraud.
- To understand how South African higher education financial aid students are affected by cyber fraud.

1.4 Rationale for the Study

South Africa has been listed as a country with one of the highest instances of economic crime in the world, with fraud identified as the most significant contributor (Mykhalchenko & Wiegratz, 2019). Financial aid is critical to enable higher education for many poor students in South Africa (Garrod & Wildschut, 2021; Wildschut-February et al., 2018), and it is crucial to understand the effect of cyber fraud on these students. Cyber fraud extends beyond financial losses and can have devastating consequences for an individual's well-being, including health issues, relationship problems, and even self-harm (Button & Cross, 2017). Individuals who have suffered losses or injuries due to criminal activity are typically referred to as victims of crime. This loss or injury can be psychological, monetary, or physical (Hussin & Zawawi, 2012).

Despite the high number of cyber fraud victims and the high cost of fraud, there is a lack of research that tries to understand how and why people become victims of cyber fraud and how it affects them (Button, 2017; Button et al., 2014, 2021a; Knüpfer et al., 2021). The effect of

cyber fraud on individuals should not be dismissed, as it can have the same effect as that of someone who has suffered from a serious crime without the same support structure (Button et al., 2014). Therefore, the effect of cyber fraud should not only focus on the monetary loss of the victim but also on their social well-being. Assessing the effect of cyber fraud on victims is essential for its intended contribution to the development or enforcement of legislation to combat cyber fraud (Knüpfer et al., 2021).

Young people often exhibit a trusting attitude towards online interactions, believing that individuals they encounter online are generally friendly and trustworthy (Du Toit et al., 2018). Therefore, investigating South African higher education financial aid students' perceptions and experiences of cyber fraud can provide insights into the extent of the problem and inform the development of strategies to prevent cyber fraud. The rationale for this study is to provide insights into the experiences of South African higher education financial aid students with cyber fraud. This information can inform the development of policies and practices to mitigate the effect of cyber fraud and ensure that financial aid students have access to safe and secure educational opportunities. Furthermore, the study can contribute to the broader research on cyber fraud and its effect on vulnerable populations globally.

1.5 Research Overview

This dissertation comprises six chapters, with Chapter 1 providing a general introduction to the study. The remainder of this paper is structured as follows: In Chapter 2, the theoretical background is derived from various research on cyber fraud and provides a comprehensive overview of the NSFAS, encompassing its role in higher education financial aid. This chapter delves into the definition of cyber fraud, exploring the factors that contribute to its occurrence and its detrimental effect on victims.

Chapter 3 outlines the research design, methodology, and ethical considerations adopted for this study, while Chapter 4 presents the results of the analysis of students affected by cyber fraud. Chapter 5, presents a discussion of the research findings, followed by a conclusion and recommendations in Chapter 6. Chapter 6 also explores the limitations of the study and suggests directions for future research.

CHAPTER TWO

2. LITERATURE REVIEW

2.1 Introduction

Cybercrime, also known as computer crime, digital crime, online crime, and other terms, has no standard definition and is a broad term that includes acts of cyber fraud. Cybercrime is any act that violates the law using digital technology, including offences such as cyber fraud, cyberbullying, cyber harassment, cyber aggression, and the distribution of illegal online content, including child pornography (C3SA, 2022; Ho & Luong, 2022).

This chapter reviews the literature on cyber fraud and its related work. It delves into the various definitions of cyber fraud and the underlying factors contributing to its occurrence. Furthermore, the review examines the landscape of financial aid within the South African higher education context and its relation to cyber fraud. Moreover, this chapter identifies the repercussions of cyber fraud experienced by its victims.

2.2 Cyber Fraud Definition

Criminals have always utilised advancements in communication to commit fraud over the centuries. From mail fraud to telephone fraud to electronic fraud. As communications have evolved, so have the opportunities and techniques of the criminals (Button, 2017). There are debates regarding differentiating cyber fraud from its traditional counterpart. A study conducted by Cassandra Cross (2019) revealed that many fraud justice professionals found no benefit from differentiating the two, as the intent and outcome were the same. Others believe there is a need to differentiate the two, as the methods and skills required to investigate the matter differ. According to Mcguire and Dowling (2013), cyber fraud can be classified as either cyber-enabled crime, where fraudsters can achieve their goals without using technological devices, or cyber-dependent crime, which requires such devices to succeed. The skills needed for cyber-enabled fraud are considerably lower than those required for cyber-dependent fraud. Emailing potential victims or setting up fake websites requires less effort than configuring malware or hacking systems (Button, 2017). Table 1 provides examples of cyber-enabled and cyber-dependent fraud.

Table 1. Examples of cyber-enabled fraud and cyber-dependent fraud (Adapted from Button, 2017)

Cyber-enabled fraud	Cyber-dependent fraud
Card Not Present Criminals use stolen card details, such as the information on a credit card, to conduct online purchases.	**Monitoring** Tools such as malware or key sniffers are used to obtain personal information. This usually requires user intervention.
Fraudulent Sales Advertising of goods or services that do not exist.	**Hacking** Systems are compromised to obtain personal information. User intervention is only sometimes required.
Phishing Attempt to get personal identifiable information with the intent to defraud.	
Advance Fee Fraud An attempt to solicit funds with promises of a bigger reward.	
Romance Fraud Manipulated victims send money to a fake online identity.	

The Institute of Internal Auditors (IIA) defines fraud as "any illegal act characterised by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force" (The IIA's, 2019, para. 2). Section 8 of the Cybercrimes Act of 2020 (Act No. 19 of 2020) in South Africa defines cyber fraud as: "Any person who unlawfully and with the intention to defraud makes a misrepresentation:

a) by means of data or a computer program; or
b) through any interference with data or a computer program as contemplated in subsection 5(2)(a), (b) or (e) or interference with a computer data storage medium or a computer system as contemplated in section 6(2)(a), which causes actual or potential prejudice to another person, is guilty of the offence of cyber fraud" (Government Gazette, 2021, p. 18).

For the purpose of this study, cyber fraud is defined as any type of fraud that uses technological devices to gain an unfair advantage, inflict injury, or induce a loss (Whitty, 2019). These types of crimes can occur either online using technological devices and the internet or offline using technological devices without the internet, or a combination of both (Kemp et al., 2020).

2.3 The Higher Education Financial Aid Context

The National Student Financial Aid Scheme (NSFAS) was established in 1999 to assist eligible students with loans and bursaries to access higher education institutions in South Africa. The Department of Higher Education and Training (DHET) is the most significant funder of the scheme, and additional contributors are the Department of Basic Education and the National Skills Fund. The NSFAS mandate was to promote equal access to HEIs, address the country's skill shortages, rectify past discrimination, and establish affordable and sustainable funding (Wildschut-February et al., 2018). Students' academic results and financial needs were evaluated to be eligible for funding. Only formal qualifications for undergraduate and postgraduate degrees were considered by the scheme at the time. In 2007, the NSFAS began funding Technical, Vocational Education and Training (TVET) institutions. The NSFAS introduced an online application pilot program in 2015, intending to become centralised and move away from disbursements being administered by institutional financial aid offices (Pillay et al., 2021). This centralised system, where students applied directly to the scheme and replaced the previous model, was called the NSFAS student-centred model (Wildschut-February et al., 2018).

This scheme has undergone several contextual transformations as presented in the subsequent sections.

2.3.1 Student Protests (#FEESMUSTFALL)

In 2015, many student protests erupted at universities due to high fees, financial exclusions, and demands for free education. This brought about the #FeesMustFall campaign and led to no fee increases for the 2016 period and fee-free higher education (Mabuza, 2020). The then-president of South Africa, Jacob Gedleyihlekisa Zuma, said that free higher education was possible but needed time to implement, which contrasted with Blade Nzimande, the Minister for the DHET, who stated that free higher education was not possible for all but only for poor students (Bitzer & Jager, 2018). In December 2017, President Zuma announced fee-free higher education for poor and working-class South African students for 2018 and beyond (Bitzer & Jager, 2018; Mabuza, 2020). This announcement by the president removed the loan component disbursed by the NSFAS and converted all student payments from 2018 onwards to a full bursary. Poor and working-class students were also redefined from households with earnings less than R122,000 to households with incomes less than R350,000 per annum. Students funded before 2018 by the NSFAS were still required to pay back the loans (Garrod & Wildschut, 2021).

2.3.2 NSFAS Funding Growth and Cyber Fraud

The NSFAS funding has grown exponentially since its formal establishment in 1999, from R441 million in 1999 (Wildschut-February et al., 2018) to approximately 42 billion in 2021/ 2022. The 2020 academic year saw funding allocated to 751,858 students, consisting of 489,912 university students and 261,404 TVET students. Female students accounted for 61.5% of the total financed students for 2020, with 470,696 female students. This is compared to 61.4% or 360,344 female students in 2018 (DHET, 2021). Figure 1 displays the total NSFAS disbursements for TVET and university students from 2010 to 2021 (NSFAS, 2022).

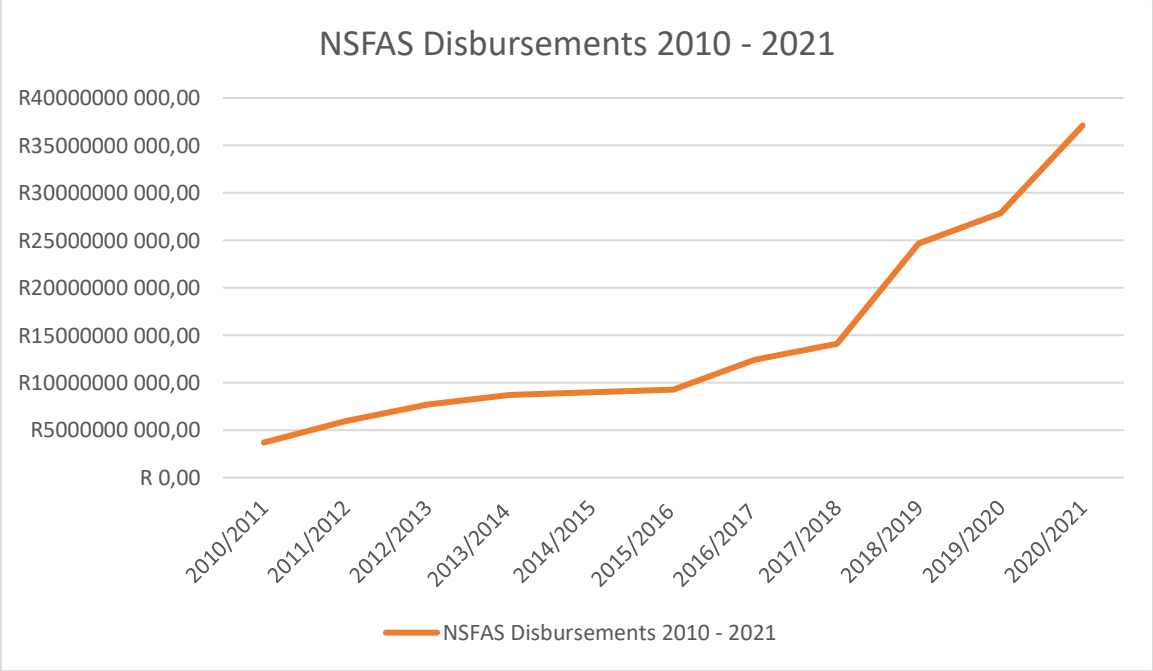

Figure 1. NSFAS Disbursements 2010 – 2021 (Adapted from NSFAS (2022))

The NSFAS bursary is available to all South Africans whose combined household earnings are not more than R350,000 per annum or South Africans with disabilities whose collective household earnings are not more than R600,000 per annum. The funding covers registration fees and tuition fees, including living allowance, learning material allowance, personal care allowance, and accommodation or transport allowance (NSFAS, 2021a). Table 2 shows the allowances for which NSFAS students may be eligible.

Table 2. NSFAS allowances for TVET and University students (Adapted from NSFAS, 2021)

TVET per annum	**University per annum**
Accommodation - urban area R24,000	Accommodation - fees charged by the university
Accommodation - peri-urban area R18,900	Transport - (up to 40 km from institution) R7 500
Accommodation - rural area R15,750	Living allowance - R15, 000
Transport - (up to 40 km from institution) R7,350	Book allowances - R5200
Transport - R7000	Incidental/personal care allowance - R2900
Incidental/personal care allowance R2900	

The NSFAS has cautioned students on numerous occasions regarding fraudsters using a variety of techniques, such as phishing, vishing, spoofed websites, and social media, to gain unauthorised access to their allowances (Bhengu, 2021; NSFAS, 2021b; Samuels, 2021). Many students receiving financial aid who were affected by cyber fraud protested against the NSFAS, claiming that their allowances, intended for their accommodation and travel, had vanished from their accounts illegally (Mbovane, 2019). Financial aid students at Durban University of Technology (DUT) also accused a staff member of defrauding them, alleging that their banking information had been altered on the portal, resulting in them not receiving their funds (Thwala, 2022).

2.4 Perceptions of Cybersecurity amongst Higher Education Students

The importance of students' understanding of cybersecurity concepts, practices, and threats is highlighted across the literature (Ahmead et al., 2024; Alharbi & Tassaddiq, 2021; Khamzina et al., 2022; Zarębska et al., 2023). Khamzina et al. (2022) recent study examining cyber security awareness among university students found no significant difference between male and female participants. Alharbi and Tassaddiq (2021) qualitative research study on the cybersecurity awareness level among college students found that more than 30% of students were not using antivirus software on their computers and that 21% were unaware of the dangers of using software from unknown sources. The online survey questionnaire was administered using the snowball sampling technique to five hundred and seventy-six (576) students who were 18 years and above at Majmaah University. Notably, 60% of the respondents used the same weak password across all their accounts as they found long or strong passwords to be bothersome. Their study also found that 22% of participants were unaware of multifactor authentication and the importance of using it (Alharbi & Tassaddiq, 2021). These findings were similar to that of Ahmead et al. (2024) and Zarębska et al. (2023). Ahmead et al. (2024) found that cybercrimes made students feel unsafe, angry, anxious, scared, and afraid. Furthermore, they found that students were not security conscience when it came to the use of social media and the internet. Given the increasing sophistication of

online threats, researchers advocate for comprehensive cybersecurity training to equip students with the knowledge and skills to safeguard themselves (Ahmead et al., 2024; Alharbi & Tassaddiq, 2021; Khamzina et al., 2022; Zarębska et al., 2023).

2.5 Factors that Lead to Cyber Fraud

The fraud triangle theory by Cressey (1953) is the most widely adopted theoretical framework for understanding why people commit fraud. Three factors are required to commit fraud. These are pressure, opportunity, and rationalisation (Wira Utami & Purnamasari, 2021). Cressey stated that for fraud to occur, all three elements must be present (Awang et al., 2021).

2.5.1 Pressure

Fraudsters are often driven to commit crimes when they feel pressured. One of the consistent pressures identified in the literature is financial hardships and this comes as a motive to commit fraud (Vousinas, 2019). Unemployment has been a significant contributor to financial hardships, especially among the youth, and is notably linked to fraudulent activities (Wakefield et al., 2022). The number of unemployed people in South Africa rose from 6.73 million (29.1%) in the fourth quarter of 2019 (Statistics South Africa, 2020) to 7.9 million (35.3%) in the fourth quarter of 2021. This is the highest level since the inception of the Quarterly Labour Force Survey (QLFS), which started in 2008 (Statistics South Africa, 2022), and is one of the highest rates in the world for urban and rural areas. South Africa also faces socio-economic challenges of high levels of inequality, low economic growth, and high poverty rates (Hlongwane & Daw, 2021). High levels of unemployment also have other socio-economic problems, such as increased crime levels or added pressure on taxpayers to cover fiscal deficits (Wakefield et al., 2022).

The unemployment issue was further compounded by the emergence and devastating effects of the Coronavirus Disease (COVID-19). For example, evidence in Washington State shows that more than one million people filed unemployment claims amid the economic turmoil brought on by the coronavirus pandemic (Baker, 2020). In South Africa, the pandemic entrenched and astronomically intensified socio-economic problems of inequality, unemployment, and poverty (Odeku, 2021). With many organisations unable to operate normally and pay staff their usual salaries, people faced financial pressures due to a lack of income, inability to pay their debts, and difficulties purchasing food (Ma & McKinnon, 2022).

These socio-economic problems contribute to triggering pressures conducive for the conduct of fraud (Wakefield et al., 2022).

2.5.2 Opportunity

According to Vousinas (2019), an opportunity refers to the fraudster's perception of being able to commit fraud without getting caught. The onset of the coronavirus disease presented an opportunity for fraudsters, as not only were many people working and studying from home, but there was also a significant rise in unemployment rates across many sectors (Ma and McKinnon, 2022). Home-based users are more vulnerable to cyber-attacks than office workers, as the technologies used to connect to the internet are less secure, with minimal firewall, gateway, and DNS protection. While most of the world's attention was focused on the pandemic, cybercriminals used COVID-19 disinformation as an attack vector to target their victims, as observed by Chigada and Madzinga (2021).

Another opportunity for fraudsters arose from human errors, negligence, and the inability to protect themselves when online. In most cases, cybercriminals need the cooperation of individuals to conduct their attacks. People can interact with the perpetrator directly by engaging in some action or indirectly by lacking adequate protection against attacks, such as outdated software or anti-malware security (Drew, 2020). People's interaction is critical in preventing attacks, such as not responding to phishing emails, opening suspicious attachments, or clicking on links, as discussed by Drew (2020). Cybercriminals target people, as they are often considered the weakest link (Hutchinson & Ophoff, 2020). This is because the skills and resources required for such attacks are lower, and the value lost per individual is smaller, making it less likely for a major investigation to be conducted as noted by Levi et al. (2015). The most common attack against human weakness is social engineering, which exploits people through manipulation and deception to extract information from victims. These attacks can occur online or offline, and have severe effects, such as financial loss, reputational damage, or both, as highlighted by Jansen van Rensburg (2018).

Criminals will use any means necessary, including exploiting victims' emotional vulnerabilities, anxieties, or psychological issues, to commit cyber fraud (Ma & McKinnon, 2022). According to Rennie Naidoo's (2020) research, the top six emotional appeals used by cybercriminals for committing cyber fraud were relief (30%), fear and hope (22% each), enjoyment (15%), threat (6%), and compassion (5%). These results indicate that cybercriminals use positive emotional appeals more often than negative ones when targeting their victims. However, it's important to note that emotional appeals are merely a distraction cybercriminals use to divert the victim's

attention from the content (Naidoo, 2020). For instance, cybercriminals may use enjoyment emotional appeals to lure victims into purchasing goods and services or exploit their goodwill by asking for donations for people in need (Ma & McKinnon, 2022).

The lack of appropriate regulations for tackling online fraud presents an opportunity for fraudsters. It is well-known that law enforcement agencies do not prioritise cyber fraud as a high-priority crime (Cross, 2019; King & Doig, 2016; Levi et al., 2015). This is due to several factors, including the lack of reporting of fraud to relevant authorities, the inexperience of police officers in combating cyber-fraud, challenges in pursuing cross-border crimes due to legislation and jurisdictional issues (Cross, 2019). While many nation-states have enacted various laws to combat cyber fraud, research indicates that it is still on the rise. Enforcing these laws is challenging due to multiple issues, such as locating criminals, collecting evidence, a lack of experts and witnesses, extradition difficulties, and international law challenges (Ajoy, 2022). As a result, cybercriminals perceive that they have much to gain, and the benefits outweigh the risks (Kimpe et al., 2020).

Developing appropriate legal frameworks for cyber fraud is usually challenged by the pace of technology. Advancements in technology have created new opportunities and techniques for criminals to commit crimes, including utilising cloud computing resources to launch various attacks. Cloud computing offers a simple registration process, resource allocation, scalability, and affordability. Unfortunately, many illicit cloud services are available for criminals to utilise, such as Hacking-as-a-Service, Botnet-as-a-Service, Malware-as-a-Service, Ransomware-as-a-Service, Phishing-as-a-Service, Backdoor-as-a-Service, Spam-as-a-Service, and Fraud-as-a-Service. The latter provides cybercriminals with tools and services to deceive their victims (Raj et al., 2021). The rise of cryptocurrencies, such as Bitcoin, has also increased cyber fraud activities across the globe in recent years. Cryptocurrencies are attractive to criminals due to their anonymity and decentralisation. These digital currencies are deemed anonymous, requiring minimal user information, and are decentralised, utilising peer-to-peer networks rather than being centralised within organisations (Trozze et al., 2022).

2.5.3 Rationalisation

Rationalisation is the justification for committing the crime and is a vital component of committing fraud. Cressey discovered that many fraudsters rationalise their misdeeds as justified, non-criminal, or not their fault (Vousinas, 2019). Criminals perceive cyber fraud as a victimless crime (Button et al., 2014; Button & Cross, 2017; Jansen van Rensburg, 2018; Ochoa Hernandez et al., 2021). They blame authorities or others for not implementing better

controls to prevent fraud. Criminals may claim that the fraud was accidental, the violation was unintentional, or plead ignorance of the law. Other rationalisations include having no direct contact with the victim, believing the victim is wealthy and does not need the money, or feeling that the victim deserved what happened due to their actions (Jansen van Rensburg, 2018). Fraudsters also justify their actions by pointing out that financial institutions usually return the funds after they have completed their investigation (Button et al., 2014).

2.6 Effects of Cyber Fraud on the Victim

Victimisation is the process of making someone a victim or the process of being victimised. Individuals who have suffered losses or injuries due to criminal activity are typically called victims of crime. This loss or damage can be psychological, monetary, or physical (Button, 2017; Hussin & Zawawi, 2012; Notté et al., 2021). Despite the high number of cyber fraud victims and the significant costs involved, there is a lack of research aimed at understanding how and why people become victims of cyber fraud and its effects (Button, 2017; Ochoa Hernandez et al., 2021). The effect of cyber fraud on individuals should not be dismissed, as it can have the same effect as that of someone who has suffered from a serious crime without the same support structure (Button et al., 2014; Knüpfer et al., 2021). Therefore, the effect of cyber fraud should not only focus on the financial loss of the victim but also on their social well-being. Assessing the emotional distress of victims is essential for its intended contribution to developing or enforcing legislation to combat cyber fraud (Knüpfer et al., 2021). The effect of cyber fraud on the victim can be classified under five key themes: financial, emotional, psychological, behavioural, and physical (Button et al., 2014; Button & Cross, 2017), which are discussed in the subsections below.

2.6.1 Financial

The financial impact refers to the monetary loss experienced as a result of fraud. This impact is usually the most obvious effect, which can have a value attached to it. It can have either minor or devastating consequences for the victim. Outcomes such as selling assets, being unable to retire due to a lack of funds, bankruptcy, or being blacklisted can become a reality for the victim. There can also be indirect costs involved, such as the time spent clearing one's name, which is estimated to be around 48 hours (Button et al., 2014; Button & Cross, 2017).

2.6.2 Emotional

The emotional effect relates to the fear experienced during the crime and the repercussions thereafter. The effects on its victims can vary in severity and duration. Some people may experience post-traumatic stress disorder or anger due to the incident (Button & Cross, 2017; Jansen van Rensburg, 2018). Tim Pascoe et al. (2006) found that identity theft fraud victims experienced agitation, distress, anger, stress, and violation. Some were concerned about the accessibility and use of their data (Button et al., 2014). In Spalek's (1999) study on the Maxwell pensioners' fraud scandal, anger was the common theme amongst victims, and the incurred loss brought about anxiety, fear, and stress.

2.6.3 Psychological

The psychological effect is where the victim's trust in groups of people or individuals has been reduced because of the association with the criminal. Some victims also feel that they are no longer in control due to the experience, with many blaming themselves (Button & Cross, 2017). Whitty and Buchanan (2016) discovered that victims who participated in their online dating scam study were more distraught about the loss of the relationship than the financial loss. Victims found the experience traumatic, and many could not cope with the lack of support from family members and friends. Denial was a key theme discovered with the victims as they could not separate the fake identity from the fraudsters or come to terms with what had happened. Victims of 419 scams were found to have feelings of disbelief and self-doubt or tend to blame themselves for unresolved fraud cases (Whitty & Buchanan, 2016).

2.6.4 Behavioural

The behavioural effect of cyber fraud victims pertains to alterations in their conduct or demeanour after the incident. This may include being more vigilant, taking measures to prevent a recurrence of similar situations, and avoiding particular activities or places (Jansen van Rensburg, 2018). For example, cyber fraud victims may become more cautious about divulging personal information online, refrain from utilising certain websites or applications, or even alter their online behaviour entirely (Button et al., 2014). Button et al. (2014) conducted a study on the effects of fraud on victims and found that changes in behaviour were either positive or negative. Their findings revealed that the incident made victims more vigilant or more security conscious, while others were less trusting of people.

2.6.5 Physical

Fraud can have physical effects on those affected by it. The negative emotions and distress caused by fraud can result in various health issues. In addition, victims may harm themselves or others they believe are at fault due to the violation. The physical effect of such crimes encompasses any health-related issues, including physical or mental problems (Button & Cross, 2017). The effects of fraud on victims, such as depression, distress, anger, and stress, can lead to physical health complications (Button et al., 2009), such as skin conditions, headaches, high blood pressure, drug abuse, or suicide (Button et al., 2014).

2.7 Chapter Summary

Fraud not only has a financial loss effect but can also have devastating effects on an individual's well-being, including issues relating to health, relationships, unemployment, and self-harm. Although prior research has examined issues of cyber fraud, there remains a gap in understanding its effects on underprivileged students. This research aims to address this deficiency. This chapter, as summarised in Table 3, examined the existing literature on the consequences of cyber fraud on its victims. The identified effects included financial, emotional, psychological, behavioural, and physical consequences. Furthermore, this chapter explored various perspectives from different authors, papers, and institutions regarding the implications and effects of cyber fraud. It also delved into the factors that motivate individuals to commit cyber fraud and the challenges in preventing and combating it. Chapter three details the methodology used to collect and analyse the data for this study.

Table 3: Literature summary

Factors that lead to cyber fraud	Pressure
	Opportunity
	Rationalization
Effects of cyber fraud	Financial
	Emotional
	Psychological
	Behavioural
	Physical
Contextual	NSFAS
	Higher education
	Demographic background of individuals

CHAPTER THREE

3. RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

In Chapter 2, an examination of the relevant literature was conducted to explore the elements that play a role in cyber fraud and its effects. This chapter focuses on the methodology and design used to investigate the effects of cyber fraud on South African higher education students who rely on financial aid. The research design is discussed in detail, encompassing the strategy and approach, sample selection and population, data collection and analysis, and a comprehensive timeline. Potential risks, ethical considerations, and confidential aspects are also addressed in the discussion of the research design.

3.2 Research Paradigm

The system of beliefs and assumptions regarding knowledge development is known as research philosophy. Burrell and Morgan (1979) assert that researchers approach their subject using implicit or explicit assumptions about their reality and how it should be viewed. In short, these are the general views about the social world the researcher holds. The paradigm should, therefore, consist of the assumptions made by the researcher about the way the research will be conducted (methodology), their idea about truth and reality (ontological stance), and what makes that truth or reality valid (epistemology) (Guba & Lincoln, 1982). Saunders et al. (2019) claim that various assumptions will be made during a research study, which could include ontological, epistemological, or axiological assumptions.

The assumptions about the nature of reality and the investigators' view on how the social world operates are referred to as ontology (Ratner, 2002; Saunders et al., 2019). It deals with the essence of the phenomena being investigated (Orlikowski & Baroudi, 1991). The two main ontological stances are objectivism and subjectivism. Objectivism believes that the researcher's subjectivity can assist them in understanding the empirical world as it exists (Ratner, 2002), that is, independent of humans. Conversely, subjectivism believes that people's perceptions and actions construct social reality (Saunders et al., 2019).

Epistemological assumptions concern the construction and evaluation of knowledge, including the best approaches for studying and understanding the empirical world and how to pass this knowledge on to others (Orlikowski & Baroudi, 1991). The types of knowledge that can be acquired and the ability to separate truth from false information are also part of these

assumptions (Burrell & Morgan, 1979). Saunders et al. (2019) list five major philosophies management researchers can adopt: positivism, interpretivism, critical realism, postmodernism, and pragmatism. Positivism is an epistemological position aiming to be objective and evidence-based. Theories are generally tested to increase the predictive understanding of the research, and measurable properties independent of the researcher or their instruments can be used. Interpretivism involves the researcher utilising their perceptions and interpretations (understanding) of the world in their research (Al-Saadi, 2014). Dependent and independent variables are not predefined in interpretive research, and the focus is on the complexity of human nature (Myers, 1997).

With this background, this study reflects on the research goal, which aims to identify and understand how South African higher education financial aid students perceive cyber fraud; and how cyber fraud affects them. Students in the higher education context who receive NSFAS are perceived as vulnerable (Garrod & Wildschut, 2021), emphasising the need to understand the experiences and effects of cyber fraud on them (IPSFF, 2020). The study adopted a subjective approach, believing people's perceptions and actions constructed social reality. It followed an interpretive approach to explore the meanings and interpretations of the people being studied (Al-Saadi, 2014), which aligned with the research objectives. Interpretivism was deemed appropriate as it concerned understanding human behaviour, such as motives and meanings, rather than predicting it (Hudson & Ozanne, 1988).

3.3 Research Approach and Purpose

This study used the inductive research approach mainly because cyber fraud within the higher education context, particularly among financial aid students, has limited coverage. Studies of this nature in emerging economies like South Africa, particularly from the perspective of vulnerable populations, are rare. When confronted with ‘contexts that are complicated or ill-defined’, inductive reasoning becomes a good alternative (Arthur, 1994), as such cases can be used to draw a general context-specific rule. This is highly needed given that most studies on cyber security tend to be from developed economies, and do not highlight the contextual needs of emerging economies.

The purpose of research can be categorised as descriptive, explanatory, or exploratory, depending on its nature. Descriptive research involves scientific methods, such as replicability and reproducibility, to observe and document a phenomenon of interest. However, this research study aimed to do more than describe the research problem. It sought to identify and

explain how students were affected by cyber fraud by identifying causal factors and their outcomes, which made the descriptive research approach inappropriate (Saunders et al., 2019).

Explanatory research, on the other hand, seeks to answer why and how types of questions by observing phenomena, problems, or behaviours for explanations. In this study, the explanatory approach was selected to understand how cyber fraud in South Africa affected higher education financial aid students. Qualitative data was collected to answer the research question. The explanatory approach best fits the criteria as the study searched for explanations of social phenomena regarding how students were affected by cyber fraud.

3.4 Research Strategy

There are various ways to classify research methods, the most common being qualitative and quantitative. Quantitative research methods use surveys, mathematical modelling, laboratories, and experiments to collect and statistically analyse data (Myers, 1997). Quantitative studies are usually concerned with numerical data, which are analysed statistically. One of the most significant benefits of quantitative studies is that quantifiable data can be generalised across large populations (Creswell, 2013). Qualitative research methods study social and cultural phenomena using methods or techniques such as ethnography, case studies, and action research. Data sources from qualitative studies can include interviews, questionnaires, observations, impressions, and researchers' reactions (Myers, 1997). Researchers observe or interact with participants of qualitative studies and are interested in explaining or exploring situations, events, or people in a natural setting (Creswell, 2013).

This research study used qualitative data collection techniques and analysis to understand how cyber fraud affects higher education financial aid students in South Africa. The study was qualitative to allow the researcher to interact with participants in their natural setting and gain insight into the effects of cyber fraud on students. Furthermore, these methods had the potential to uncover additional information regarding the students' perceptions of cyber fraud that other research approaches may not have captured. The study adopted a case study approach to gain deeper insights into the higher education context. The study sought to understand how South African higher education financial aid students perceive cyber fraud; and how cyber fraud affects them, given the existing research gap. A case study was deemed appropriate as it focused on answering 'how' and 'why' questions, a defining feature that allowed for an in-depth examination of a specific case. The case study approach also allowed the researcher to seek uncovered constructs, gathered the experiences or context of

participants' actions, and understood the effect of cyber fraud on students (Bhattacherjee, 2012).

3.5 Population and Sampling

Sampling is the process of selecting a portion of a population to study or analyse that population. It is crucial that the sampling process is representative of the population and is done correctly and in a balanced way, as it is not feasible to study entire populations due to resource constraints (Patten & Newhart, 2017). The first step in the sampling process is to define the target population, which could be people, a continent, a company, an object, or any other analysis unit that one wants to study. This is followed by selecting a sampling frame, which is the location or information where the target population can be found. The final step is to select a sample using a well-defined technique, such as probability sampling or non-probability sampling (Bhattacherjee, 2012). In probability sampling, each unit of the population has an equal chance of being selected through random selection. In contrast, in non-probability sampling, the population has a zero chance of getting selected due to the researcher's bias, judgement, and convenience. Non-probability sampling is targeted at a specific group, and the researcher understands the broader population is not represented (Patten & Newhart, 2017).

Two sampling methods were used for this study. The first method was purposive sampling, which targeted specific individuals with knowledge or experience related to the topic being studied. A non-probability sampling method was selected because not all financial aid students had been victims of cyber fraud, and participants could not be selected randomly from the sampling frame. The selection of participants relied on the researcher's judgement (Saunders et al., 2019). The second approach was a snowball sampling technique, which involved asking identified respondents to recommend other higher education financial aid students affected by cyber fraud. This was also a non-probability sampling technique, and the chances of being selected for participation could not be accurately determined (Bhattacherjee, 2012).

The goal of this research study was to recruit higher education financial aid students who had been victims of cyber fraud. After obtaining ethical clearance, the researcher requested permission from the National Student Financial Aid Scheme (NSFAS) (Refer to Appendix C) to obtain a list of students who had been victims of cyber fraud. The NSFAS is a government entity and is one of the largest student financial aid providers in South Africa for tertiary education. Students who were victims of cyber fraud reported these fraudulent activities to the NSFAS to prevent further transactions by fraudsters on their accounts. During the introductory

meeting, the researcher explained the nature of the research, its procedure, and potential benefits, and asked permission to obtain a list of students from the NSFAS who had been affected by cyber fraud. The NSFAS permitted the researcher to contact students affected by cyber fraud (Refer to Appendix D).

3.6 Data Collection

The data collection process used a qualitative method for data collection. In qualitative research, data sources could be anything from texts, objects, individuals or groups, organisations, and environments (Cooper & Schindler, 2014). Interviews are the most popular choice for case studies and interpretive research, as other methods, such as direct observations and field notes, can supplement them. This research study used semi-structured interviews with open-ended questions as the research instrument for data collection. Semi-structured interviews are considered natural forms of participant interaction compared to quantitative methods such as surveys. Interviews using the interpretive research approach attempt to create an environment of openness and trust where participants can express themselves freely (Saunders et al., 2019).

A list of non-exhaustive questions was created before the interview using key concepts from existing academic literature to guide the conversation. These sensitising concepts, as seen in Appendix G, were gathered using the following resources: Abdulai (2020), Agrafiotis et al. (2018), Button et al. (2021a), Button and Cross (2017), Lazarus et al. (2022), and Ma and McKinnon (2022). Additional questions were asked if the participants needed to address the research question in their narratives. For example, if a student forgot to mention what emotional effect they experienced during or after the incident, they were asked to elaborate if they had experienced any. Cyber fraud may affect students in various ways, and their perceptions about it could differ from one student to another. Hence, this study used semi-structured interviews as an appropriate research method. This approach allowed for flexibility, as specific questions could be left out or added, and the order of questions could be adjusted based on the natural progression of the discussion. This allowed the researchers to gather the necessary information to answer the research questions and objectives. Saunders et al. (2019) support this approach.

All interviews were conducted telephonically over two months, from February to April 2023. Holt (2010) argues that telephonic interviews have many advantages for narrative research, such as interviews can be done remotely, cost-effectiveness as the other party does not need to pay, convenience for both parties and the potential to elicit greater details during narrative

responses. Semi-structured active interviews were conducted with participants to understand their experiences and knowledge about cyber fraud. Holstein and Gubrium (1995) state that active interviews are a collaborative process and more effective than traditional interviews in retrieving the lived experiences from respondents. This can be achieved using various techniques, such as probing, mirroring, summarising, and silence (Holstein & Gubrium, 1995). The interviews were recorded with the participant's consent and transcribed. Open-ended interviews and discussions about cyber fraud lasted between 15 and 39 minutes (M = 22 minutes). The sample selection process introduced a bias towards reporting victims, as only those who reported the fraud to NSFAS were interviewed.

Although telephone interviews offered convenience for both the researcher and participants, in-person interviews would have been better suited for this type of research due to the sensitive nature of the topic and the participants' experiences with cyber fraud. Several students exhibited scepticism towards the interviewer, responding cautiously and revealing minimal information, possibly due to concerns about the study's legitimacy or the fear that the fraudster, who had their contact information, might seek additional details. Despite a comprehensive explanation of the study's purpose, some participants remained distrustful, which is understandable. Participant SABCF_004, for instance, voiced their doubts after the questionnaire, asking: "*How did you get hold of my information*"? Other students who expressed distrust of the interviewer include Respondents SABCF_010 and SABCF_011, who remarked: "*Even you, it's not like I trust you fully*" and "*I still can't trust anyone who asks me personal questions like you. I just do not trust anyone at the moment*". Similarly, Participant SABCF_016 stated that they are more vigilant, explaining: "*Even now, I'm curious about this phone call*" and at the end of the interview, asked: "*Mhh, is this Legit*"? Furthermore, after the interview, Participant SABCF_017 raised concerns, asking: "*Since we have done the interview, are you going to tell people from my institution*"?

3.7 Data Analysis

After collecting the data, each interview was transcribed using the transcription feature in Microsoft Word. This feature converts audio recordings to text, saving the researcher a significant amount of time. The researcher then carefully listened to each transcribed interview to verify its accuracy and ensure it aligned with the interview experience. The transcripts were securely stored, and password protected on UCT's OneDrive cloud platform, with access only granted to the researcher and their supervisor. The research employed Braun and Clarke's (2006) thematic analysis method to analyse the data. This method is iterative and does not follow a linear progression. Thematic analysis is a popular qualitative method that offers

flexibility, ease of use, and the ability to identify similarities and differences across data sets, making it an appropriate tool for policy development (Braun & Clarke, 2006).

The data was analysed using NUD*IST Vivo (NVivo), a freely available computer-assisted qualitative data analysis software (CAQDAS) for UCT students. NVivo is well-suited for both qualitative and mixed-method research and uses a qualitative approach to analyse qualitative data. This approach involves identifying, linking, and coding themes or concepts to test or build theories or explanations (Lewins & Silver, 2009). The researcher followed the six phases proposed by Braun and Clarke (2006) for analysing the qualitative data.

The researcher familiarised themselves with the data. The interview audio recordings were transcribed into Microsoft Word documents. Creswell (2013) emphasises the seriousness of respecting participants' privacy and safety by using aliases or pseudonyms to protect their identities. All participants were assigned an acronym and a corresponding number depending on the order in which they were interviewed. The acronym used was SABCF, which stands for Student Affected By Cyber Fraud. An example of this would be: If the student were the third interviewee, their identifier would be SABCF_003. The researcher thoroughly reviewed the transcribed data to become familiar with the content, and any initial ideas were written down. Initial codes were generated by capturing keywords or phrases identified during a thorough reading of the transcribed data. Some codes were created deductively, using the sensitising concepts, while others were created inductively by identifying patterns in the data. For example, SABCF_004 expressed dissatisfaction with the assistance received from the NSFAS, mentioning: "*I felt that there wasn't anything more they could do, and it is how they operate*". Similarly, SABCF_006 stated: "*They didn't do much to help me, corruption has always been there*", leading to the creation of an initial code: "Assistance received satisfaction".

The data was organised and categorized in a meaningful way with coherent identification and naming of themes. For instance, SABCF_001 had initial codes like "college," "police," and "Financial aid institution" as they reported the fraud to these institutions as explained by SABCF_001 who said: "*I went to the institution and the help person just told me that I must carry on calling NSFAS […] I went to the police station. The police station also told me the same thing that I must carry on calling the NSFAS. […] That's what I did, which I got help, yes"*. Similarly, SABCF_003 expressed: "*I report the matter to the police station, then I open the case. […] I reported to the college and the NSFAS*". SABCF_007 reported the matter to their institution and the NSFAS but not the police as explained: "*I reported to NSFAS, and I reported at the institution. I did not think about reporting to the police station*". These codes were grouped under the theme "cyber fraud incident reporting".

The themes were reviewed to ensure they were consistent with the data, provided a comprehensive summary of the findings, and accurately represented the data. For example, further analysis of the theme "Realization of fraud" revealed that the subtheme can be organised into a distinct category: "events or circumstances". The themes were clearly defined, free from ambiguity, and directly supported by the data. For instance, the theme “Time Spent” was defined as “To understand the amount of time the student spent attempting to resolve the cyber fraud incident”. Once the themes were identified, the findings were presented clearly and concisely.

3.8 Research Timeframe

The research was designed to be cross-sectional to understand how cyber fraud affected higher education financial aid students in South Africa at a single point in time. Cross-sectional research designs are commonly used when researchers aim to collect data on multiple cases to identify patterns of association (Bryman & Bell, 2011).

3.9 Resources and Project Plan

The researcher used technology to conduct interviews whenever possible, such as through MS Teams, Zoom, telephone, or Google Meet. The researcher accepted full responsibility for covering all expenses, including unanticipated costs. Table 4 includes the project plan with actionable tasks and expected completion dates. The study was completed by October 2023.

Table 4. Research project plan

Task	Due Date
High-Level Research Proposal	17 March 2022
Literature Review	01 May 2022
Dissertation proposal	14 June 2022
Present Research Design	08 August 2022
Research Design	26 August 2022
Apply for Ethics Committee	November 2022
Approval from Ethics committee	November 2022
Data Collection & Analysis	November 2022 - June 2023
Dissertation Write-up	July 2023 – September 2023
Presentation of Dissertation	October 2023
Submission of Dissertation	November 2023

3.10 Project Risks

Research projects face many risks, such as ethical, technical, and participation failures (Saunders et al., 2019). Due to the topic's sensitive nature, students may have felt overwhelmed by the emotional pain of reliving or discussing the cyber fraud they experienced,

and they may choose to withdraw from the research study. The researcher demonstrated compassion to the students during the interview process and allowed them to withdraw from the study or reschedule if the process became overwhelming. In addition, students were given the option to receive support from a UCT trauma counsellor during the interview process. The researcher allocated sufficient time for data collection and analysis, as shown in Table 4 above. The researcher also began the data collection process after the ethics clearance was approved.

During the data collection process, the researcher considered four factors: response error, response bias, interviewer error, and interviewer bias. Response error was defined as any factor that could negatively affect the participant's performance, such as interviewing them in the morning when they had other things to do rather than later in the day. Response bias was defined as any factor leading to inaccurate responses, such as interviewing participants in an open office where colleagues or friends could overhear their responses and make them uncomfortable. Interviewer error refers to any factor that could affect the interviewer's interpretation of responses, such as conducting interviews with all participants in one day, leading to researcher fatigue and potential data errors. Finally, interviewer bias was defined as any factor that could introduce bias in how responses were recorded, such as interpreting the responses subjectively (Saunders et al., 2019).

3.11 Ethics and Confidentiality

Ethics is concerned with protecting participants, researchers, and the organisation or institution under which the research is conducted (Babbie et al., 2015; Saunders et al., 2019). Creswell (2013) posits that researchers must ensure that the participant's rights, values, needs, and desires are always respected. Participants should knowingly consent to participate in the study without manipulation, deceit, fraud, or duress (Creswell, 2013). The participants' identities should be protected by ensuring that only the researchers involved in the study, who are committed to maintaining confidentiality have access to the information. Potential risks and impacts of the study should be clearly outlined to the participants as they could be emotionally or physically harmed, ridiculed by the information they provide, or have their friendships and family relationships affected (Babbie et al., 2015).

The Commerce Faculty Ethics in Research application form was completed, and ethical approval was sought from the University of Cape Town's Ethics Board before conducting the research study (Refer to Appendix F). The study followed UCT's Commerce Ethics in Research Handbook and Policy. Before the interview process, participants were given a cover

letter (refer to Appendix A) and a consent form (refer to Appendix B). Participants were informed about the purpose of the research, the type of data collected, the anonymity of the data, the ability to withdraw from the study at any time, and other important information. Due to the study's sensitive nature, the interviews could potentially force students to relive traumatic experiences related to cyber fraud. Participants were offered the option to receive support from a UCT trauma counsellor during the interview process. Personal details and statements were anonymised to protect participants' privacy. The collected data was kept in a secure location that was password-protected and accessible only to the researcher and the researcher's supervisor.

3.12 Chapter Summary

This chapter has outlined the methodology framework employed for data collection and analysis for the research study. The study adopted a qualitative research design and employed purposive and snowball sampling techniques to select participants for the research. A semi-structured interview instrument was used to guide the conversation, and a set of non-exhaustive questions, informed by key concepts from existing academic literature, was developed before the interviews to guide the discussions. The sample consisted of 30 NSFAS beneficiaries, all of whom had experienced cyber fraud. Thematic analysis was applied to analyse the gathered data, facilitating a deeper understanding of the effect of cyber fraud on South African higher education financial aid students and their perspectives on the issue.

The subsequent chapter will provide an in-depth exploration of data analysis and the resulting findings.

CHAPTER FOUR

4. ANALYSIS AND FINDINGS

4.1 Introduction

This research utilised qualitative research methods to address the following research questions:

a) What are South African higher education financial aid students' perceptions of cyber fraud?
b) How are South African higher education financial aid students affected by cyber fraud?

The study used an inductive approach to theory and qualitative methods for data collection. Interviews were the primary method used. Thematic analysis was used to analyse the data collected in the software tool NVIVO to identify and extract the relevant themes. The following subsections present the analysis key findings and a comprehensive discussion of the implications of the study.

4.2 Descriptive Findings

4.2.1 Demographic descriptors

The goal was to interview higher education financial aid students who had fallen victim to cyber fraud, aiming to understand their perceptions and the effect of cyber fraud. The largest provider of financial aid for higher education students, namely the NSFAS, was contacted, and they provided the researcher with contact details to invite students to participate in the research study. During the interview process, participants were also asked if they knew of any other higher education financial aid students who might have also been victims of cyber fraud.

Out of the list of students provided by the NSFAS, the researcher contacted 144 students before data saturation was reached. Data saturation is a point in qualitative research were gathering additional information no longer provides new insights or information (Saunders et al., 2019). Of these, 43 went to voicemail and were not called back, 21 did not answer, and no further attempts were made to contact them. Forty-nine (most of whom were males) expressed disinterest in the study. When asked for their reasons, most cited suspicion of us being fraudsters or not believing the study to be real, while others mentioned being too busy. From the remaining 29 successful participants, one participant referred us to a classmate who had also been a victim of cyber fraud. This information was verified using the provided list from NSFAS of affected students.

Out of the 30 respondents, four were males (13.3%), 24 females (80%), and 2 participants who preferred not to answer (6.7%). Their ages ranged from 18 to 34, with an average age of 23. Seventy percent (70%) of the total respondents were between 18 and 24 years old, 17% were between 25 and 30, and 13% were between 31 and 36 years old. Most participants had a home/first language that was not English. The most common first language among the respondents was isiZulu, with 43% (13 students), followed by isiXhosa with 17% (5 students), and Sepedi with 13% (4 students). English, Sesotho, and Xitsonga each had 7% (2 students). Setswana and siSwati both had 3% (1 student). The National Qualifications Framework (NQF) classifies and describes the various qualifications and educational levels in South Africa. There are 10 NQF levels, with level 1 being the lowest and level 10 being the highest. The last six levels are higher education qualifications. Higher Education Institutions may recognise alternative forms of prior learning for admission if applicants do not meet the minimum entry requirements, provided they can demonstrate the necessary competence (DHET, 2007). Thus, student who might only have NQF level 2, may still be eligible to apply for admission to Higher Education Institutions.

Students' highest level of education ranged from NQF level 2 to NQF level 6. One student (3%) reported having NQF level 2, six students (20%) stated that they have NQF level 3, seventeen students (57%) had NQF level 4, three students (10%) had NQF level 5, and three students (10%) reported having NQF level 6 qualification. In terms of geographic location, most of the participants (9 students) interviewed were from KwaZulu-Natal, followed by Gauteng Province with five students, Eastern Cape and Limpopo with four students each, Mpumalanga and Free State with three students each. North-West and Northern Cape had one student each. All respondents confirmed that they had been victims of cyber fraud and experienced financial losses. Table 5 provides a detailed breakdown of the participant demographics.

Table 5. Interviewees Demographic Characteristics

Participant	Gender	Age	Education	Location	Home Language
SABCF_001	Female	22	NQF Level 4	KwaZulu-Natal	isiZulu
SABCF_002	Female	25	NQF Level 2	KwaZulu-Natal	isiZulu
SABCF_003	Male	23	NQF Level 4	Limpopo	Sepedi
SABCF_004	Male	24	NQF Level 4	KwaZulu-Natal	isiZulu
SABCF_005	Male	25	NQF Level 4	Limpopo	Sepedi
SABCF_006	Female	26	NQF Level 4	KwaZulu-Natal	isiZulu
SABCF_007	Female	24	NQF Level 6	Eastern Cape	isiZulu
SABCF_008	Female	23	NQF Level 4	Limpopo	Sepedi
SABCF_009	Female	22	NQF Level 4	Gauteng	English
SABCF_010	Prefer not to answer	24	NQF Level 5	Northern Cape	Setswana
SABCF_011	Female	24	NQF Level 3	Gauteng	siSwati
SABCF_012	Female	31	NQF Level 4	KwaZulu-Natal	isiZulu
SABCF_013	Female	21	NQF Level 4	Gauteng	isiXhosa
SABCF_014	Female	23	NQF Level 3	Eastern Cape	isiXhosa
SABCF_015	Male	23	NQF Level 3	Limpopo	Sepedi
SABCF_016	Female	20	NQF Level 4	Free State	Sesotho

SABCF_017	Female	23	NQF Level 3	Mpumalanga	isiZulu
SABCF_018	Prefer not to answer	34	NQF Level 5	Eastern Cape	isiXhosa
SABCF_019	Female	24	NQF Level 6	Gauteng	Xitsonga
SABCF_020	Female	21	NQF Level 4	Mpumalanga	Xitsonga
SABCF_021	Female	31	NQF Level 6	KwaZulu-Natal	isiZulu
SABCF_022	Female	27	NQF Level 4	Eastern Cape	isiXhosa
SABCF_023	Female	23	NQF Level 5	KwaZulu-Natal	isiZulu
SABCF_024	Female	31	NQF Level 4	Gauteng	English
SABCF_025	Female	20	NQF Level 3	Mpumalanga	isiZulu
SABCF_026	Female	19	NQF Level 4	North-West	isiZulu
SABCF_027	Female	26	NQF Level 4	KwaZulu-Natal	isiXhosa
SABCF_028	Female	22	NQF Level 4	Free State	isiZulu
SABCF_029	Female	21	NQF Level 3	KwaZulu-Natal	isiZulu
SABCF_030	Female	22	NQF Level 4	Free State	Sesotho

4.2.2 Preferred Device for Internet Access Among Students

The results indicated that most students (97%) preferred accessing the Internet through their mobile phones, as seen in Table 6. They mentioned convenience as a critical factor, with respondent SABCF_012 stating: "*Yeah, actually, I am used to a phone, so I feel more comfortable when using a phone. Because I can go wherever with it*". For others, it was simply a personal choice, as explained by respondents SABCF_012 and SABCF_019: "*Even though I have a laptop, I prefer using my phone*" and "*Sometimes I use my desktop, but most of the time I use my phone".* Some students mentioned limited data access as a hindrance to using other devices, such as respondent SABCF_017: "*I do have a laptop, but because of the data I can't use it*". This sentiment was shared by respondent SABCF_018: "*Yes, I just prefer using my phone; there is no internet connection where I live, I just buy data to access the Internet*". For a few students, their mobile phone was their only means of accessing the Internet as they had no other devices. Only one student, SABCF_025, preferred to use a laptop to access the Internet.

Table 6. Overview of Device Preferences and Internet Accessibility among Students

Variable	Item	Count	Percentage
Device Preference	Mobile Phone	29	97%
	Mobile Tablet	0	0
	Computer Desktop	0	0
	Laptop	1	3%
	Other	0	0
Internet Accessibility	Easy	14	47%
	Difficult	11	37%
	Mixed	1	3%
	Prefer not to answer	4	13%

4.2.3 Internet Accessibility

Students were asked to describe the ease or difficulty they experienced accessing the Internet. The results are represented in Table 6. Many students (47%) found it easy to access the Internet; these students did not rely on mobile data but had access to Wi-Fi, fibre, or ADSL connections. However, 37% of students needed help accessing the Internet. They cited high mobile data costs as a significant obstacle. For instance, respondent SABCF_008 mentioned, "*most of the time I cannot afford the data or airtime to access the internet*", and SABCF_018 added, "*Yoh it's not easy at all because I have to buy my own data to access the Internet. So, without data I don't have access to the Internet*". Additionally, poor network coverage in their rural areas posed difficulties for students like respondent SABCF_012, who stated, "*It is quite difficult to access the internet because I live in the rural areas*", and SABCF_014 expressed, "*I find it difficult for me to access the internet, most of the time in rural areas we have poor network coverage*".

4.2.4 Internet Usage

Most students used the Internet daily, except for respondent SABCF_007, who used it weekly. SABCF_007 found it challenging to access the Internet without assistance; in their statement, they mentioned: "*When it is easy for me is when I get someone who knows the internet to help me and sometimes when I am alone, I find it hard to have access to the internet, so I leave it just like that*". Students mentioned using the Internet for various purposes, including research, learning, online shopping, communication, job searching, social media, and entertainment. For example, respondent SABCF_004 emphasised the cost-effectiveness of online shopping, stating: "*With online shopping it is because of discounts*". Respondent SABCF_005 highlighted the convenience of online shopping, stating, "*Online shopping, because I can purchase wherever where I am at, I do not have to go to the store, I do not have to travel, I do not have to, you know what I mean. I am just sitting down and then order. After 3 days ,7 days that's when my order comes in*".

Respondent SABCF_006 found social media to be a helpful source of information, stating: "*It is sometimes, because I need more information from other groups*". This sentiment was echoed by respondent SABCF_007, who said: "*Reason being that I tend to learn more things because social media is a worldwide thing. You get to know what is happening worldwide inbound and outbound*". Respondents SABCF_021 and SABCF_022 mentioned that they use social media for job searching, with SABCF_021 mentioning: "*Facebook pages are relevant to seeks jobs*". SABCF_018, identified as a programmer, uses the Internet to communicate with other developers and solve problems as explained: "*I develop websites so most of the*

time I like, when I have a problem. I just log in, there are platforms like stack overflow, GitHub and all that so, I use the Internet most of the time to communicate with other developers on those platforms and do research just need something that I don't know. I have to research it online".

4.2.5 Security Measures

Students were asked what security measures they have to protect themselves and their devices from online threats. Various strategies were reported, including using passwords or security codes, regular software updates, and utilising antivirus software. Respondent SABCF_001 mentioned a practice of not saving credentials while logging into websites and ensuring her phone is locked after use, stating: "*you see when you're logging in, then there will be a point where you have to save the password or saying no saving and locking my phone every day*". On the other hand, respondents SABCF_004, SABCF_010, SABCF_016, SABCF_027, and SABCF_028 acknowledged that they take minimal or no precautions to safeguard themselves against security threats.

4.2.6 COVID-19 Lockdown

The COVID-19 lockdown period proved challenging for students, as they could not attend school and were confined to their homes. Accessing mobile data became difficult as many businesses were restricted from operating. During this period, students were asked to evaluate their experiences, and those with easy internet access considered it a positive experience. Conversely, students who could not purchase data due to lockdowns or financial constraints found it to be a negative experience. They reported that the colleges did not provide them with data for online learning during the pandemic, necessitating them to find their own means.
Respondent SABCF_017 mentioned needing to seek assistance to access the Internet for their studies, stating: "*No, I wasn't affording it, I would even ask my mom to hotspot me*". Respondent SABCF_014 found it difficult, noting: "*It had a negative impact because my mom who was doing part time jobs at the time, and lost her job. She was the one who was assisting with buying data*". Similar sentiments were shared by SABCF_008, who said: "*Yoh it affected me bad because, uhm, it has been a bad experience hence I couldn't access my academics, and I missed out a lot*". SABCF_024 also found it challenging to access the Internet, stating: "*Because at that time, I couldn't go to school and my husband salary got cut. so financially we couldn't we afford it at that time. So, for the data we had to buy like daily bundles just to get do homework for my daughter and stuff like that. So, it was a lot of struggles*". On the other

hand, some students had a positive experience during this period, like Respondent SABCF_021, who explained: "*I got to learn new stuff*".

4.3 Students' Perceptions of Cyber Fraud

This subsection focuses on the students' perceptions of cyber fraud. Using interviews with students affected by cyber fraud, we try to understand students' perceptions of cyber fraud. We start by looking at what students think cyber fraud means and their knowledge of the topic.

4.3.1 Cyber Fraud Knowledge

The respondents were asked what their understanding of the term cyber fraud or online fraud was, as seen in Figure 2. It should be born in mind that the higher education institutions together with the NSFAS have repeatedly sent information regarding cyber incidents to the public and particularly to students on how to protect themselves, as well as reporting fraud (https://www.nsfas.org.za/content/preventfraud.html). For example, students had been warned by NSFAS to be vigilant when using payment platforms due to the disturbing levels of cyberattacks (Mashale, 2023; Matlhabe, 2023).

The findings show that 25 (83%) of the respondents interviewed knew or could explain what it was. Respondent SABCF_001 described cyber fraud as "*fraud, like, when fraudsters are using computers or Internet where they able to take your money or your things*". (SABCF_001). Similarly, SABCF_003 and SABCF_004 perceive the term to mean "*occurs online*" (SABCF_003) and "where a person's information is stolen online" (SABCF_004). Notably, SABCF_005 defines it as a scam where individuals fall victim to deception through technological means: "*It is sort of a scam, where you sort of scammed technologically*". At the same time, 5 (17%) of respondents did not know or could not explain the term cyber or online fraud such as SABCF_027: "*No, I've never heard of it. It's the first time*"; however, they were aware of terms such as scam, fraudsters, and fraud. Many students who knew the term cyber fraud, had learned about it through personal experiences such as having friends, family, or acquaintances who were victims of cyber fraud.

4.3.2 Cyber Fraud Training

Most respondents (90%) indicated a lack of training in cyber fraud, as illustrated in Figure 2. Only 3 (10%) individuals reported receiving formal training. Three individuals said they learned about cyber fraud as part of their coursework. SABCF_011 took a cybersecurity course and

said: "*Yah, I once did cybersecurity, I think it is similar. I am doing levels right, there is life Orientation, life skill and computer literacy*". SABCF_018 also learned about cyber fraud in their IT course, which was part of their curriculum. They said: "*I was studying something that is related to IT Internet and all that. So, it's part of the curriculum, the cyber fraud, all that cyber bullying and all that*". On the other hand, SABCF_014 indicated that they encountered the concept through their business studies, explaining: "*I learnt about it through business studies. There would be sections of fraud*".

The rest of the respondents learned about cyber fraud through various other means, such as social media, word of mouth, friends, and Google. Respondent SABCF_030 explained: "*I was reading some novel, and I came across that term. My friend once forwarded me some information on cyber fraud".*

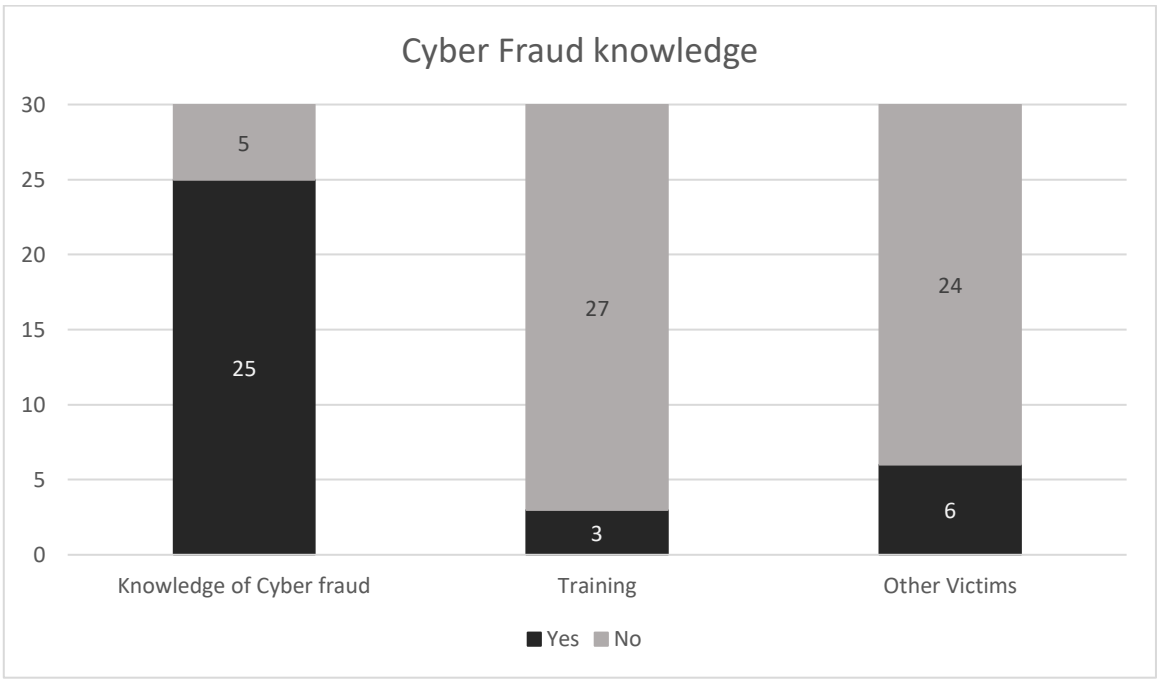

Figure 2. Cyber Fraud Knowledge

Some students also learned about cyber fraud after becoming victims themselves. It should be noted, however, that the majority (80%) of respondents said they did not know anyone who had been a victim of cyber fraud. 20% stated that they were aware of other students who had become victims. Two respondents, SABCF_013 and SABCF_020, shared that they have heard about others who have been affected by cyber fraud but do not know them personally. SABCF_013 said, "*it was people from campuses*", and SABCF_020 said, "*Yes, I have heard of others".* Several respondents knew other victims of cyber fraud. SABCF_019's roommate was a victim. Similarly, SABCF_022 knew Someone who experienced the same situation as them. SABCF_025 knew Someone who was a victim of SIM card fraud, in which money was

stolen from their bank account, and SABCF_029 knew someone who was defrauded and dropped out of college.

4.4 Perceived events that led to cyber fraud

This section explores the events or circumstances that led to the cyber fraud incident. Students were also asked to provide more information on how they reported the incident, to whom they reported it, and the support they received. Additionally, students were requested to provide background information on how they applied for bursaries to study at the college.

4.4.1 Online Application for NSFAS Fund

All students applied for their bursaries online through the NSFAS portal. Eleven students applied independently, while the others sought assistance at the college where they planned to study. Two students asked family members for assistance with their applications, two got assistance from strangers at an internet cafe, and one received aid from a stranger at the library. Upon registering, and having an account, students were able to detect some strange activities such as when they could not log into their accounts.

For example, Respondent SABCF_005 stated: "*I wanted to check through my NSFAS portal, my password and all of that were not working like it didn't want to open*". Other students realised they were victims when they tried to reset their passwords, and the contact details were incorrect. For example, Respondent SABCF_002 said: "*Everything that was there was not mine*", referring to the contact information, and Respondent SABCF_009 shared: "*When I change my password it then said that it sent a password to a different e-mail that I don't know of. It is then that I realised that I was being defrauded here*". Some students realised they were victims after receiving notifications that their account information had been updated or their accounts had been blocked. For example, Respondent SABCF_008 explained: "*It came to my realisation that I was hacked when I received a notification that someone got through my NSFAS account*", and Respondent SABCF_006 said: "*When I had to withdraw the money, I couldn't because it kept saying blocked*".

Other students realised they were victims after logging in to find their accounts empty. For example, Respondent SABCF_013 recounted: "*I realised when I logged in to find an empty account. That's when I realised that I was a victim*". Respondent SABCF_001 said: "*I started to know that there's been fraud because I never received the money, I never took the money out so that's where I know its fraud*". Respondent SABCF_019 explained: "*I logged into my*

account and transferred R1000 so that I could withdraw it. Then I stayed almost like 3 days not withdrawing anything. From there I noticed that there was a zero balance on my account. At that point, I realised that I'd been scammed".

4.4.2 Pretexting and Pharming

Most students pinpointed social engineering as the primary source that led to cyber fraud incidents. Pretexting involves impersonating a legitimate entity, in this case, posing as an NSFAS employee. Vishing, a type of voice communication pretexting, was used on Respondent SABCF_010 and Respondent SABCF_024. SABCF_010 recounted: "*This person said he was from NSFAS, and they noticed that I am struggling to do a transaction. Because I was struggling, I even forgot that you shouldn't give anyone your password. But the way he was talking to me, I was convinced that he works for NSFAS. I thought he was going to help me*". Similarly, respondent SABCF_024 explained: "*Someone phoned me, and I didn't know that NSFAS don't phone. They only communicate via e-mail, SMS, or something, but they don't phone. So, I didn't know at that time*". Furthermore, Respondent SABCF_026 was tricked by a fake NSFAS social media page, as they stated: "*Yeah, it was on the NSFAS page. I thought it was a legal NSFAS page. Only to find out that it's not. So, I gave them details, the ID number and the name and surname. Yeah, everything*".

Pharming attacks using lookalike websites that resemble the NSFAS student login portal emerged as a prevalent method through which students fell victim to compromised login credentials. These websites were designed to look and feel identical to the official NSFAS portal and wallet websites. Students reported encountering these misleading links on the social media pages of fake NSFAS groups and their respective colleges' social media pages. Respondent SABCF_021 vividly recollects the incident: "*There was a group on Facebook for our college. There were links that were sent to the group. So, I opened the link using my details and I realised that the link was to get my details so that they can generate vouchers without my knowledge*". Similarly, SABCF_019 had a similar experience: "*I remember going through Facebook and going to my institutions Facebook page. I got the link there and filled in my personal information*". In yet another case, Respondent SABCF_013 sought assistance within a NSFAS Facebook group and was deceived by someone pretending to help: "*There are groups on Facebook, you'll find students seeking help on the comment section. So, I also commented, and then there was this one person who responded with a link for us to use, and I used the link. Little did I know that it was a scam*".

Three respondents, namely SABCF_011, SABCF_017, and SABCF_025, believe that Someone assisting financial aid students at the institution may be involved. Respondent SABCF_011 distinctly recalls leaving their login credentials with an individual assisting at the

student support office. They needed help with their application, and the person assisting them was another student who eventually faced suspension. SABCF_011 explained, "*I remember, there was a time that I went to SSS (Student Support) because I usually do not have data. Remember, they see most people like they don't know how to use computers. So, they suggested that we just leave our personal details there. You know as students we trust each other*". Furthermore, Respondent SABCF_017 distinctly remembers the sole occasion when they shared their credentials, which was for assistance at the student support centre. They recollected, "*I only went to student support and explained my issue. They told me that I should write my details and after that, I never received my allowance*". Respondent SABCF_025 suspects that someone at the institution they studied at may have misused her ID to compromise her login credentials. She expressed her suspicion, saying, "*I suspect the institution. They do have our information and all the details*".

Respondents SABCF_015 and SABCF_022 suspect that individuals close to them may have been involved in the fraudulent activities they experienced. SABCF_015 recalled, "*I remember my sister trying to assist me with receiving the money, I can say yes, I told someone my details*" and she further added, "*I think she did it herself*". SABCF_022 expressed a similar sentiment, stating, "*I think that the person that did this is someone that who knows me. Because my password was so careless, it was my date of birth*". Financial theft by Someone close is not uncommon, as exemplified by a recent article detailing the case of a NSFAS student who incurred a loss amounting to R21,680 from her allowance, perpetrated by individuals she considered to be close friends (Mashale, 2023). Another respondent, SABCF_014, acknowledged that she provided her login details to someone online when she needed assistance. She explained, "*It usually happens on Facebook. I think I shared my details with someone when I was desperate for funding*".

Moreover, SABCF_018 believes that their credentials may have been compromised by a Telegram group they belonged to. SABCF_018 described the situation, saying: "*So there was this group on Telegram that I joined for programming stuff and all that you know. I suspected that they had stolen my number from that group. There was this theme of connecting to the Internet or seeing stuff that's connecting to the Internet for free without buying data. Yeah, yeah, I know, I know that is fraud that I was doing. I joined the group because I needed the Internet at that time. So, I think, one of them, or whoever in that group stole the numbers of the members of this group, and then you know what people are doing when they have your information, such as name and number and all that*". When asked to clarify how they might have gotten the password, SABCF_018 continued: "Let's *say on my portal, I registered with my phone number all my data, cell, phone number, e-mail, and all that. So, in that group, we must join in with your e-mail and cell phone number. When they have your e-mail and*

telephone number, it's easy to get information about you. Especially when you are using your phone because there are cookies, cookies you know store your data. So that's what they did, I think".

Three respondents, SABCF_023, SABCF_029, and SABCF_030, were unsure how their accounts were compromised. SABCF_029, in particular, stated: "*That's one thing I couldn't figure out. I am still wondering if maybe they used an ID number or maybe I gave someone my phone at school, and they used my phone. I honestly do not know what happened*".

4.5 Perceived Effects of Cyber Fraud

4.5.1 Financial and Time Loss

Funds earmarked to assist students with their accommodation, transportation, and personal expenses were stolen from them. As shown in Figure 3, the minimum loss per student was at least R1,000, with the maximum exceeding R10,000. Five students reported losing more than R1,000, nine incurred losses exceeding R5,000, and eleven lost more than R10,000. Many students were unsure of the exact amounts they were supposed to receive because they had not been provided with contractual documentation specifying their allocated amounts. Consequently, some students only became aware of the extent of the fraudulent deductions upon successfully contacting the NSFAS contact centre, while others only learned the amounts when they regained access to their login portals.

Five students were unsure of the exact amounts taken from them, as elucidated by respondent SABCF_011, who expressed: "*I went on months without getting my allowance. It was tough. I didn't know how much I was supposed to get*". Similarly, SABCF_014 explained: "*I think I have lost a lot of money. I am not sure what was my monthly allowance as that was never shared with us. Students used to get different amounts. Some students get R18,000 for the month of January to June and others R10,000*". Respondent SABC_016 also described a similar situation, saying: "*I don't know how much got at that time. So, I can't say how much I lost. It depends, because as college students, if you apply for accommodation, you get about 10,000. If you applied for transport, it's about 5000 per semester*".

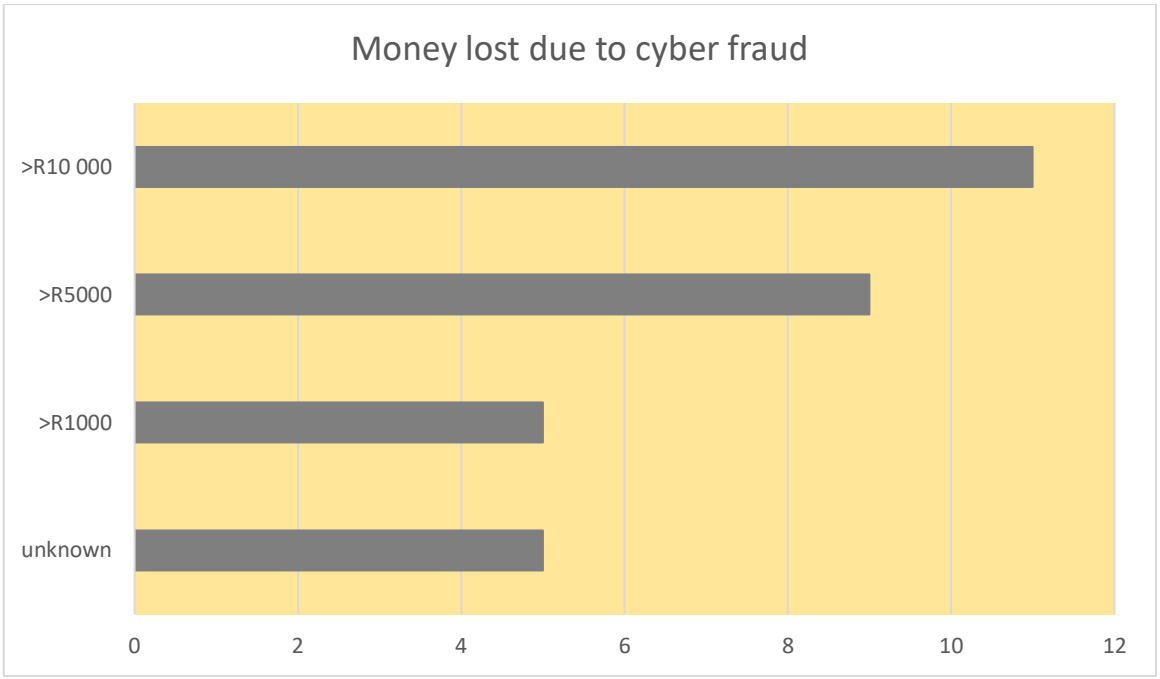

Figure 3. Money lost due to cyber fraud

The NSFAS dedicated fraud hotline, which is run by an independent company called Vuvuzela Hotline (Pty) Ltd, is often the first point of contact for students who call the NSFAS contact centre for assistance with a fraud-related matter, as explained by participant SABCF_027: "*I called NSFAS. They gave me a Cape Town hotline number to report fraud*". While the NSFAS contact centre telephone number (0800 067 327) is zero-rated for students to call, the Vuvuzela fraud hotline (0860 247 653) is not. It is essential to highlight that the NSFAS presents the Vuvuzela fraud hotline as a toll-free number on its official website, as indicated in Figure 4 below (NSFAS, 2023). In reality, this hotline has associated charges, as explained by participant SABCF_028, who incurred additional airtime costs to call: "*Maybe like R150. The money I used was to buy airtime and NSFAS takes time to answer*". The researcher verified this by calling the Vuvuzela fraud hotline on October 6, 2023, using a prepaid and a contract SIM card. In both cases, the calls consumed airtime and deducted minutes from the contract sim, indicating that it was not a toll-free number.

In addition to the financial hardships mentioned earlier, students had to find additional funding to address the various expenses associated with their travel costs or accommodation, food, and personal expenses. Many students turned to their families and friends for financial assistance despite their families struggling financially. Additionally, some students resorted to borrowing money they would eventually need to repay. For instance, one of the participants, identified as SABCF_009, shared their experience, stating: "*I had to ask my sisters, friends, to assist me. Because even though I was getting allowance from home, it wasn't enough. I*

think I've borrowed about R10,000, to try and cover for that money". Another respondent, SABCF_013, found it difficult to disclose the circumstances surrounding their financial request to their family. They explained: "*I was supposed to buy food with that money, I asked them back home to send me money. I didn't tell my family of the incident; I just told them that I needed money. After some time, I was then able to talk about it*".

Participant SABCF_011 relied on a friend for assistance, explaining: "*There is nothing as painful as people receiving their allowance and you are not. I had a friend at that time that I was saying with an she was helpful. Even though she wasn't complaining, I could tell that it was also difficult for her. She was doing almost everything for me*".

Figure 4. NSFAS depicting Toll-free Fraud hotline (NSFAS, 2023)

Apart from the financial loss, students highlighted the time it took to address the cyber fraud incident. Among the 23 respondents who shared their experiences regarding the duration required to regain access to their accounts, the collective average stood at 6.7 months, as illustrated in Figure 5. One student, SABCF_001, recollected: "*It was a lot of time, I used to go to the police station. I used to go to central for my school, just to find out what's happening*". Another student, SABCF_006, was unable to resolve the issue and dropped out of school. They explained, "*Almost 2 years fighting the same issue. I did not get any help. It was difficult to get to school*". Similarly, Respondent SABCF_007 also endured a two-year struggle and said: "*I kept going to the bursary office, but I did not get any help. I just gave up*". Students found the recommended steps by law enforcement to be lengthy, as explained by Respondent SABCF_018: "*Yes, I did go to the police station. I did follow the steps that they said I must follow. So, I spent a lot of time trying to resolve the case*".

Many encountered difficulties when attempting to contact the NSFAS for assistance. Respondent SABCF_018, recalled: "*I have sent a lot of e-mails to NSFAS trying to unblock my account. I would call only to find that I am number 30. So yes, it is a lot of time*".

In addition to the time spent trying to resolve the fraud, students also incurred out-of-pocket expenses, such as data costs for e-mailing the NSFAS and travel costs to visit the institution and the police to follow up on their cases. These additional expenses varied widely, with one student spending as little as R30 and another spending as much as R3000. For instance, Respondent SABCF_018 explained that their expenses were low because they were living in a residence near the college and the police station. They said, "*It's not a lot of money, maybe R15 to the police station and R15 back*". However, other students were not so fortunate, as articulated by Respondent SABCF_005, who said: "*I lost R1800 because of the traveling. Mind you, where I live it is far from my institution*". Respondent SABCF_017 similarly reported a financial burden, estimating: "*I think I lost about R2000-R3000. I live far, so I would pay around R600 for transport. Then also spending on data*". One student, Respondent SABCF_021, travelled to another province at his own expense to try to investigate his case. He explained: "*For calls, I would use their toll-free number. I only used the money to travel to the college. There was a time when I went to Durban to try and find the person who withdrew my money at the store. I did not succeed because of the procedure involved when it comes to requesting CCTV footage in store*".

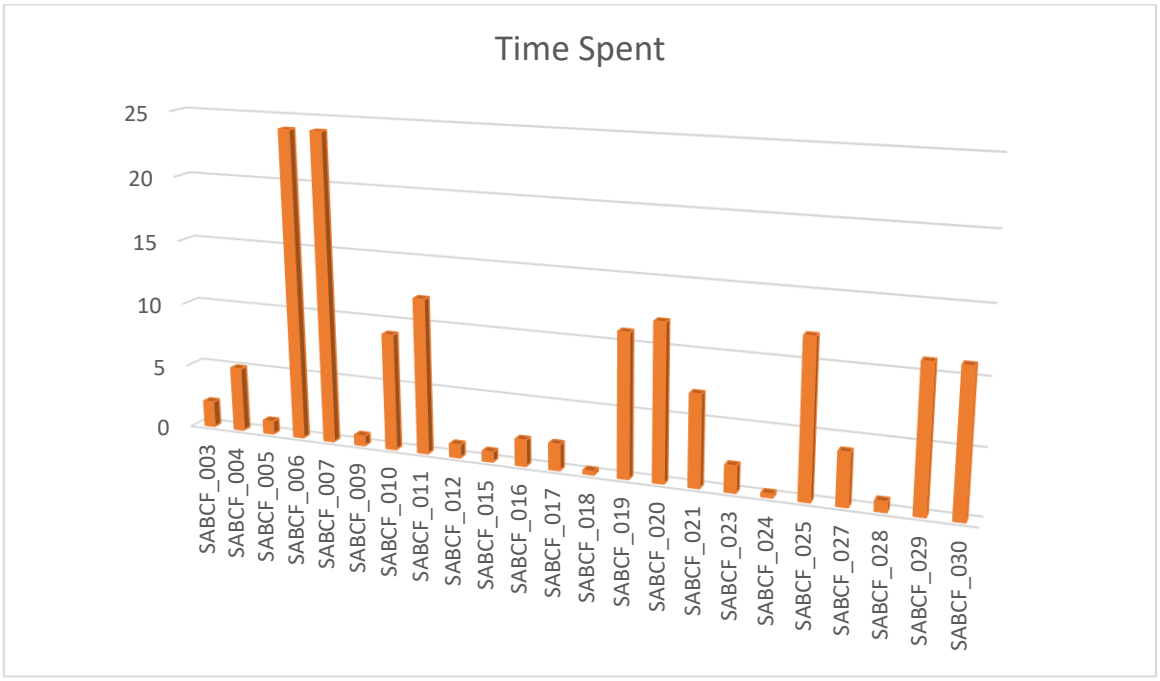

Figure 5. Time spent

4.5.2 Loss of Trust in the NSFAS and Legal System

Once students lost their NSFAS funds through cyber fraud, most opted to report to the authorities. 40% reported the cyber fraud to the police, 80% reported it to the college, and 87% reported it to NSFAS, as depicted in Figure 6. Certain students encountered relative ease when reporting incidents to the police and obtained a case number, such as respondent SABCF_003, who remarked: "*I report the matter to the police station, then I open the case. They gave me the case number*". Likewise, SABCF_018 indicated: "*I did get the case number and yeah, they followed the case but just didn't produce any good results*", and SABCF_024 shared: "*The police officer was very chilled with me. He explained everything. He was patient. So, it was easy for me to open one*".

In contrast, other students found the process of reporting cyber fraud to the police to be complicated. For example, respondent SABCF_001 stated: "*The police station also told me I must carry on calling the NSFAS, they couldn't give me the case number until you confirmed that this is a fraud. They gave me the affidavit paper. So, I didn't go back there*". Respondent SABCF_005 recounted: "*I went to the police station first. They told me to bring the proof. I had screenshots, I went to the printing shop and photocopied those things. I then went back to the police station. They did not open a case for me, they just told me to leave the papers and come back. They never came back to me*". Respondent SABCF_010 conveyed their frustration by explaining: "*I went to the police station to open a case. They said when did this happen? I said yesterday. They asked me where was I at that time? I said Kuruman. They then told me it is not their case; I should go open a case at Kuruman. They then said that they can open a case for me, but they would transfer it to Kuruman. Every week I used to go to the police station to check the person who was busy with my case, and they would say he was not there. They called after a long time, and they told me that there was nothing they could do and they are closing the case*".

Sixty per cent of students did not open a case, citing reasons such as not thinking of it at the time or the process being too long. For instance, Respondent SABCF_021 articulated: "*I was told to open a case of which I didn't because it was a lengthy process*". Respondent SABCF_023 did not report it to the police, stating: "*There were others who reported it to the police but did not get help, so I did not see the need to report it*". Meanwhile, Respondent SABCF_027, who had inadvertently entered his login details on a fraudulent link that mimicked the NSFAS portal, did not report the matter to the police, reasoning: "*I didn't know what to tell the police. These people used my details, so I couldn't think of a way to explain it*".

Twenty-four students (80%) reported the incident to the college. Many of the students who reported the matter to the college did not have much success as they were often told to contact the NSFAS, such as the case with respondent SABCF_008, who remembered: "*I tried reporting it to the college yes, and they told me to call NSFAS*". Respondent SABCF_007

remembers: "*I reported at the institution. The bursary office didn't even do a follow-up, I always go to the bursary office. They just told me to bring my ID copy, always. I always go to the police station to certify my ID and submit it to the bursary office*". Respondent SABCF_014 also reported the matter to the school, but after waiting a year for the matter to be resolved, gave up as explained: "*Yes, we went to report the matter at school, but it was never attended to. So, I decided not to continue with school". Respondent SABCF_016 also reported the matter to the institution but felt that the college was not interested in assisting them, as explained: "The college didn't even bother*".

A segment of students who refrained from reporting the incident to their institution had various reasons for doing so. Some believed that reporting the matter to NSFAS and the police would suffice, as explained by Respondent SABCF_022: "*I thought that since there was NSFAS fraud and the police, I didn't know that it was a must to tell the institutions*". On the other hand, respondent SABCF_013 opted not to report the incident to the institution due to feelings of embarrassment. They recalled, "*No, I didn't report it. After two weeks of the incident, the institution sent communication about the fraud, but it was too late. I was ashamed to say that it happened to me*".

Twenty-six students reported the incident to NSFAS. Many found the process difficult, citing reasons such as difficulty reaching a representative or enduring extended waiting times. For instance, one respondent mentioned, "*I called them, and the response that I got was that their offices are currently busy*". Respondent SABCF_010 shared a similar experience, noting: "*I used to call NSFAS every day and get that automated response saying that I am number 158*".

Conversely, students who refrained from reporting the incident to NSFAS cited similar reasons for their decisions. For example, respondent SABCF_014 stated: "*No, I did not, I just gave up*" when asked if they reported the incident to NSFAS, and respondent SABCF_015 expressed: "*No, I tried calling the NSFAS office, but they didn't take my call*".

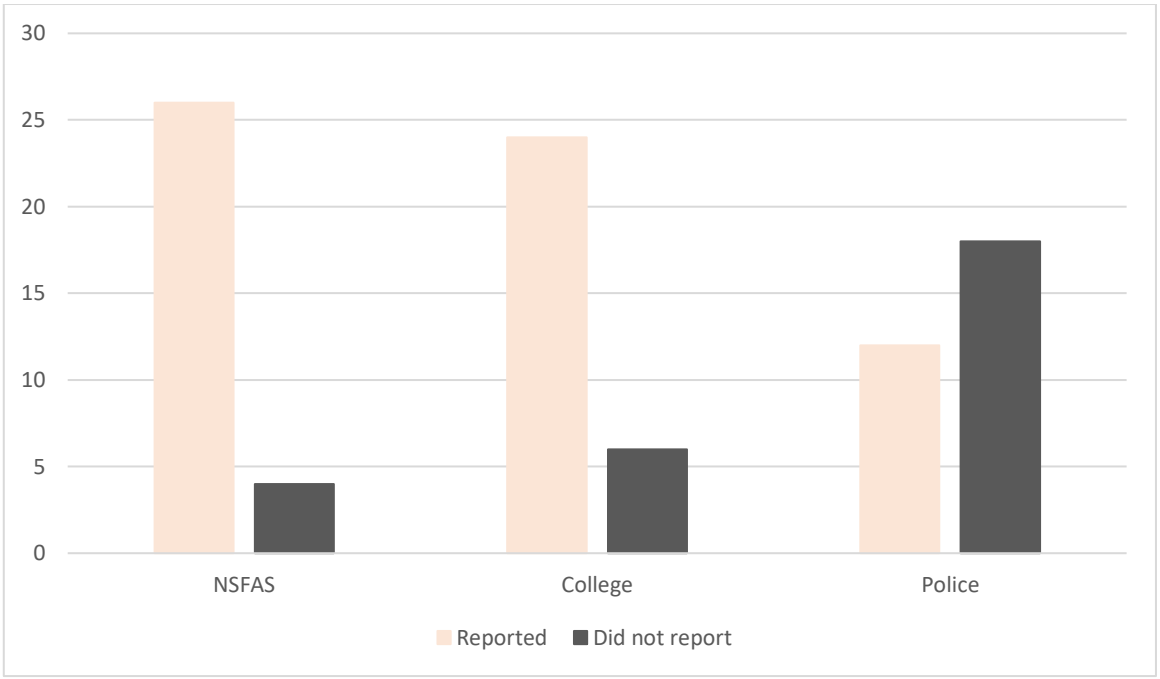

Figure 6. Fraud Reporting

All students affected by cyber fraud did not receive their stolen money back, and none of the reported fraud cases filed by students at the police station led to arrests or successful outcomes. While some students regained access to their accounts, others did not. Respondent SABCF_008 managed to resolve their problem with accessing their account on their own, as they could not get assistance from NSFAS. Similarly, Respondent SABCF_010 also faced challenges obtaining assistance from NSFAS, explaining: "*They didn't do anything. They should have blocked my account completely, you know, but they didn't. So, what is the point of calling NSFAS if they won't help*".

Respondents SABCF_015 and SABCF_016 believed that the college and NSFAS could have aided affected students more proactively. SABCF_015 remarked: "*They never assisted me actually*", while SABCF_016 added: "*The college and the police didn't even bother and the NSFAS, I think if they could be more reasonable when you write e-mails, they should explain further what's happening and what not. Other than us writing e-mails for nothing*". Respondent SABCF_025, unfortunately, received assistance later than needed. When asked about the recovery of their account, they explained: "*Yes I managed, but after a long time, because I ended last year, I dropped out, because of school fees, transport and rent*". However, there were more fortunate students such as SABCF_023 and SABCF_027, who successfully regained access to their accounts. SABCF_023 confirmed, "*Yes they did assist me, and my account was unblocked*". At the same time, SABCF_027 stated that despite the prolonged

wait, their account was eventually reinstated, explaining that: "*I did get help, the people that blocked my account, they had to re-register my account*".

Survey respondents were queried about their satisfaction with the support they received from the college, NSFAS, and the police. Their responses varied. Respondent SABCF_004 expressed satisfaction with the college's response: "*I felt that there wasn't anything more they could do, and it is how they operate*". Respondent SABCF_005 believed that the police could have been more proactive, stating: "*I can't say the police, because at the police station I was at was not active. So, as for school they helped me to fight*". Respondent SABCF_019 echoed a similar sentiment about the police, mentioning: "*No, because they never got back to me to tell me that they managed to trace the people that did this. I did not get my breakthrough*". Respondent SABCF_006 expressed dissatisfaction with all three entities, remarking: "*They didn't do much to help me, corruption has always been there. It is difficult to trust them*". Similarly, Respondent SABCF_008 expressed a lack of trust in all three entities, stating: "*I lost trust in all of the above, because I feel like people like us who are poor get easily tricked and not helped when they need help*".

Respondent SABCF_012 felt that the NSFAS bursary office could have done more, recounting: "*I feel that the lady from NSFAS could've assisted me rather than saying she can't help me. I went three times to the lady at the institution, but she didn't assist me*". Respondent SABCF_013 believed that both NSFAS and the college could do more to safeguard students from social engineering attacks, explaining: "*I feel they could have done more; there are so many links out there. They could do more to stop this from happening*". SABCF_017 shared a similar viewpoint, commenting: "*They could've done more to assist me*". Respondent SABCF_020 felt they did not receive much help from the police or the college but eventually received assistance from NSFAS, saying: "*I did not get any assistance from the police station. I opened a case, but I was later told that the case was closed because there were no leads. At the college, I was told to leave my details, but I never received any feedback. NSFAS did get to a point of assisting me*". Respondent SABCF_024 felt that the college was unhelpful but did receive assistance from NSFAS, stating: "*No, I didn't get any help. They just told me to phone NSFAS, it has nothing to do with them*".

Respondent SABCF_027, although pleased that her school fees were still being paid despite not receiving her allowances, believed that NSFAS could have been more responsive, expressing: "*They could have done more by responding in time. Because I needed those funds, and I was struggling*". Respondent SABCF_029 attributed the delay in assistance to NSFAS systems, remarking: "*The financial aid tried to assist me, I think it's their system that is not quick enough*". Finally, Respondent SABCF_009, who successfully regained access to

their account, felt that NSFAS had done enough, explaining: "*I feel that they have done enough because if I wasn't able to regain my account, I would say that they didn't do anything*".

4.5.3 Social and Institutional Support

Students who were victims of cyber fraud received various support and assistance, both formal and informal. Some students received emotional support from friends and family members, while others received more practical support, such as help with accommodation or financial assistance. For example, respondent SABCF_004 recollected receiving emotional support from friends and assistance from a family member who provided travelling fare to attend college. In their words: "*I got help from other students; they managed to comfort me, and that way, I didn't think a lot about it till things got better*". Similarly, Respondent SABCF_005 remembered experiencing anger but credited their friends with helping them. They said: "*By keeping my friends around because they were making me happy, making me forget about what happened to me. They were buying me food because I had no money. I had nowhere to sleep at that time. So, they accommodated me until I healed*". Respondent SABCF_006 recounted their struggles with the lack of funds for the school but mentioned receiving support from both their partner and their child's grant money. They explained: "*I was using my child's grant money and my partner was also supporting me*".

Respondent SABCF_012's situation was particularly trying as they came from a child-headed family. They had to endure long walks to school due to a lack of funds. They shared: "*I am basically the elder in my family. I would walk long distances because of not having money for transport. Whether it is raining or not, I still need to walk to school. There was no one in the family that could help me*". Respondent SABCF_017 received comfort from a stranger. They explained: "*I spoke to this other lady who comforted me, and she explained that I am not the first and I am surely not the last. She would check on me every day because I had even lost weight because of the fraud incident*". One lecturer played a pivotal role in assisting Respondent SABCF_018 in dealing with the cyber fraud incident. In their words: "*There is a lecture there at school. He was teaching me data communications and networking. He helped me to get through that situation*". Respondent SABCF_025 disclosed that counselling sessions and the support of their boyfriend were instrumental in helping them cope with the difficult period they faced. On the other hand, Respondent SABCF_024 found strength in their husband and daughter, which allowed them to move forward. Lastly, Respondent SABCF_029 discovered that staying active and surrounded by people contributed to their resilience during this challenging period.

4.5.4 Emotional Effects

Anger and stress were the dominant emotional effects of cyber fraud on students, including self-directed anger, frustration with the circumstances, and disappointment in the institutions they feel have failed them. Respondent SABCF_001 described their emotional state, stating: "*I was angry for my institution that they weren't able to like, help me. I'm asking the assistant, why don't you call them? I'm here, just help me. You call them. Maybe they'll answer because they will see that this number is coming from the institution*". Respondent SABCF_007 felt hopeless, explaining: "*I can say that I had anxiety, I was feeling emotional and sad at the same time. I am funded but I am not getting my allowance. It affected me badly, I felt like I'm losing hope on that*". Likewise, SABCF_008 shared a similar sentiment, expressing: "*Yoh it was a bad experience, It was very traumatic. I lost hope. I felt angry and lost faith*". Respondent SABCF_009 expressed concern about potential eviction from their accommodation, saying: "*It has caused me stress because I had to figure out how I was going to pay for my accommodation*". Along the same lines, SABCF_026 faced accommodation-related challenges due to this incident, explaining: "*It was stress as I did not have stable accommodation and all that*".

Respondent SABCF_018 emphasised the financial dependence on the stolen funds, explaining: "*Stress, because at home, I'm living alone. My mom and dad passed away. So that money was making a huge difference in my life. So now they stole it. Things started to fall apart. I couldn't focus, I couldn't give my 100% focus on the study*". Similarly, Respondent SABCF_023 found it challenging to concentrate on their studies due to heightened stress, stating: "*I was very stressed, it was even difficult to even focus on my studies*". This cyber fraud incident exacerbated the anxiety of an already anxious respondent SABCF_019, as they elaborated: "*I already had anxiety, so matters got worse. I would sometimes feel like I am running out of breath. I would just wake up midnight*". Participant SABCF_016 was concerned about the challenges of returning to school, expressing: "*Stress and anxiety of how I will get back to school*".

Participant SABCF_027 also grappled with depression due to concerns about covering transportation costs to school and accommodation, explaining: "*Yoh, depression, because, yeah, I couldn't sleep. I had to think about money for transport and accommodation*". Finally, SABCF_025 struggled with anger issues and academic setbacks, remarking: "*I had anger issues because I did not write my exams. I couldn't cope, even now. I couldn't study last year because they said I failed my modules*".

4.5.5 Psychological Effects

The psychological effects of cyber fraud on individuals can manifest in various ways, with students often facing significant challenges in dealing with the aftermath. In the study, 90% of students reported that their trust in people or institutions diminished after experiencing cyber fraud as illustrated in Figure 7. This included trust in friends, family, the government, and online platforms. SABCF_011 expressed a loss of trust in these institutions, stating: "*I do not trust anyone. A person will promise you something but instead do the opposite*". Respondent SABCF_002 described the effect of the cyber fraud on their life, saying: "*Yes it changed me, I don't trust anyone now, I don't do anything with people, I just struggle on my own if I don't know anything*". Similarly, participant SABCF_018 echoed these sentiments, expressing: "*I can tell you that experience changed my life. Even today, I have a problem trusting people*". Furthermore, students who fell victim to online social engineering attacks shared their diminished trust in online platforms.

SABCF_008 described a significant loss of confidence, especially in online activities, explaining: "*I lost confidence a lot, even now, I do not trust anything, especially online stuff, I have lost trust*". SABCF_010 expressed fear and scepticism, citing a prior hacking incident: "*I am now scared. Someone called me from Vodacom, and I was like nah you want to scam me. Someone once hacked my Capitec account before NSFAS. I was like, I cannot trust anyone*". Participant SABCF_012 admitted mistrust of social media platforms, stating: "*I honestly do not trust online platforms, especially Facebook*".

A trend of self-blame emerged among the participants during the interview phase of the study. To investigate this further, the researcher asked the remaining 14 participants if they blamed themselves for the cyber fraud incident. The outcomes of these inquiries are illustrated in Figure 7, wherein 78% of the individuals interviewed reported blaming themselves. Noteworthy responses from this subset of participants offer valuable insights into their perspectives. Respondent SABCF_015 articulated: "*I can put the blame on myself, I could have done it myself, but since I was not able to do it, that's why I wanted to ask for help*". Participant SABCF_017 shared: "*I blamed myself a lot, I regretted writing my details on that paper provided at the student support*". In a similar vein, participant SABCF_018 expressed: "*I do somewhere somehow. Because, if I didn't join that Telegram group, maybe that thing was not going happen*". Respondent SABCF_019 conveyed that initially, self-blame was predominant, stating: "*At first I blamed myself. I was asking myself why did I even go online to access those things. As time went by, I realised that I was not the only one, because we are not educated on these things. I thought NSFAS was more secure*".

Respondents SABCF_020 remembered: "*Yes, I did blame myself. If did not use that link, I wouldn't have been scammed*". Participant SABCF_021, on the other hand, recognised self-

blame but found it unproductive, stating, "*I did blame myself, but it wasn't helping. I am that kind of person who faces challenges head-on*". Respondent SABCF_022 expressed regret for using their birthdate as a password, admitting: "*I blame myself for that password, I just wish I tried something else than my date of birth*". In contrast, SABCF_023 interpreted the experience as a valuable life lesson, remarking: "*I did not blame myself. I just learned the hard way that I should never give my personal details to anyone*". Participant SABCF_024 exhibited mixed feelings regarding self-blame, reflecting: "*You know what I do, but you know, I also don't. Because at that time, I didn't know. It was my first year, my first time using it. So, I didn't know anything*". Finally, respondent SABCF_026 evolved in their perspective, noting: "*I did at first, but now no. I just told myself that it was never my fault, it was them*".

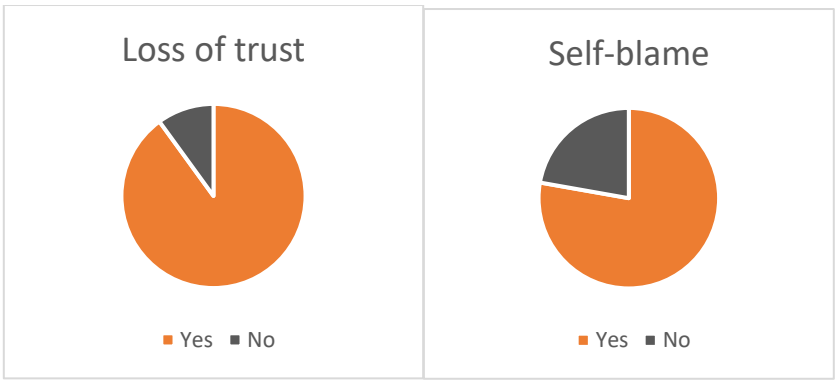

Figure 7. Loss of Trust and Self-blame

4.5.6 Behavioural Effects

All participants interviewed exhibited behavioural changes after the cyber fraud incident. The majority of participants reported a heightened sense of vigilance, particularly in relation to social media, phone calls, interactions with suspicious URLs, and the sharing of personal information. Some participants even went so far as to warn others about obvious online scams. Notable examples of this proactive behaviour were observed with participants SABCF_019 and SABCF_021, who described their experiences as follows. Participant SABCF_019 conveyed: "*Now, I'm even more vigilant. I used to warn other students, like don't, don't, don't. Don't go through links you do not know. Do not even entertain them. Cause even now they do send those links. And, I'll make sure, I'll comment; Do not even try to do that*". Participant SABCF_021 elaborated on their proactive approach in their school's Facebook group by stating: "*All I did was post in the group that they should be aware of the scam. I warned them about the links and, also suggested to the group admin that they should check links that are posted in the group, and people with obvious fake profiles should be removed from the group*". Other notable behavioural changes of participants include participant SABCF_001 implementing a more secure approach to their online activities. They no longer store their login credentials on any device and refrain from using other people's phones to log in. This shift in

behaviour was explained as follows: "*Asking someone can I log into your phone and check my status? No, I don't do that anymore. I don't save my information online or on my phone too, just log in and log out when I'm done*". Participant SABCF_009 has become increasingly vigilant when identifying fake URLs, stating: "*Right now I'm very cautious about which site I visit*". Respondent SABCF_018 has exhibited a heightened awareness of security, particularly about social media. They have taken proactive steps to enhance their online safety, remarking: "*I just changed my password for everything on my phone, my e-mail address password, everything. I deleted whatever group that I joined on Facebook, I blocked the people that I'm not sure of, or I don't know*". Additionally, Participant SABCF_024 has adopted a more cautious approach when confronted with phone calls or SMS's, explaining: "*When it comes to phone calls or SMS's, especially when it's from NSFAS, I will go to my classmates and ask did you also get the SMS or, did NSFAS also phone you? If they say no, then I know it's that time again, let me not answer it*".

4.5.7 Effects of Cyber Fraud on Student's Education

The study participants were surveyed regarding the effect of cyber fraud on their education. Responses ranged from minor to no effect to more significant consequences, such as affecting academic performance or even dropping out of school. Out of the 30 students who participated in the study, 26 provided information on the effect of cyber fraud on their education. Of these 26 students, 16 were affected, which is represented in Figure 8 below. The effect on education percentage was calculated in Table 7 as 16 students affected out of 26, with a percentage of 62% (rounded to the closest digit). Ten students confirmed that the cyber fraud did not affect their grades or their ability to pass, nine students dropped out of school, and seven had their grades affected.

Ten students (38%) whose pursuit of education remained unaffected by the cyber fraud incident can be attributed to a combination of factors, such as good emotional support structure, stable financial support, minimal financial losses from the fraudulent incident, and determination to succeed despite the challenges. One participant, SABCF_011, whose financial loss is uncertain, contemplated dropping out of their studies but found inspiration and strength from a friend who reminded them of their challenging home situation, explaining: "*My friend used to tell me that I should always think about my home situation, which is something that gave me strength to go on*". Similarly, participant SABCF_024 (lost R11,000), whose husband assisted her financially during the incident and whose daughter was her source of strength, remarked: "*To become a policewoman and to do what I always wanted to do, so that I can provide for my family. That was my motivation*". Another respondent, SABCF_013, who suffered a financial loss of R1,000, sought assistance from family members back home.

Meanwhile, SABCF_016, uncertain about their financial loss, received financial assistance from their uncle. Other students who managed to overcome the cyber fraud incident without significant academic setbacks include SABCF_020 (lost R2,000), SABCF_023 (uncertain about their financial loss) and SABCF_028 (lost R7,700). These individuals relied on a parent for financial assistance, with SABCF_023 sharing that despite completing their final year, it was not easy, as explained: "*I was stressed, I was very stressed, it was even difficult to even focus on my studies*".

A total of nine students, constituting 35% of the participants, did not complete their studies and dropped out of the course. They cited various reasons for this decision, primarily revolving around challenges related to attending school, such as transportation costs and the expenses associated with food and accommodation. Among those who dropped out, financial constraints were the main issue for the students, with specific students such as SABCF_002 (uncertain about their financial loss), SABCF_006 (lost more than R10,000), SABCF_017 (lost R11,000), SABCF_022 (lost R11,000), and SABCF_030 (lost R7,000) highlighting transportation costs as the problem. For instance, SABCF_002 articulated: "That's *why I didn't pass, I was not going to school on a daily basis*". Additionally, participants SABCF_008 (lost more than R5,000), SABCF_010 (lost more than R8,000), SABCF_015 (lost more than R6,000), and SABCF_025 (lost R10,000) were unable to meet the costs associated with accommodation, leading to their decision to withdraw. SABCF_025 explained: "*I did not have money to pay rent and buy food. So, I decided to drop out*".

Furthermore, participant SABCF_030 initially received some support from family members and friends but expressed discomfort with relying on them, stating: "*My sister would try and assist. I would also ask my friends for assistance. It did not sit well with me. It used to give me stress, thinking that I had to bother my family to assist me*". Lastly, SABCF_025 added that they had no one at home who could financially assist them.

Seven students, representing 27% of the participants, reported that the cyber fraud incident had a negative effect on their academic performance. These individuals attributed the decline in their grades to heightened stress levels, including SABCF_009 (lost R9,000), SABCF_004 (lost more than R5,420), SABCF_026 (uncertain about their financial loss), and SABCF_029 (lost more than R5,000). Respondent SABCF_004 stated: "*It affected all my tests. I didn't write well*", and SABCF_009 expressed: "*My grades dropped because I was under a lot of stress*". Participants SABCF_029 and SABCF_026 received financial assistance from a parent at home. Participant SABCF_009 resorted to borrowing money to offset the stolen funds. At the same time, Participant SABCF_019 (lost more than R14,000) managed to persevere with the financial support of her father and boyfriend, as explained: "*It affected me a lot. Like my*

studies, it was hard for me to come to terms with the fact that I lost so much money. I even thought of dropping out". Participant SABCF_027 (lost R4,000) faced challenges attending classes due to financial constraints, which had an adverse effect on their grades, as explained: "*Sometimes I couldn't attend classes because of money, and lessons were continuing*". Respondent SABCF_018 (lost R14,000), received emotional support from a lecturer who felt that the cyber fraud incident hindered them from achieving their desired academic performance, expressing: "*I didn't pass with the marks that I wanted. So, it affected me a lot*".

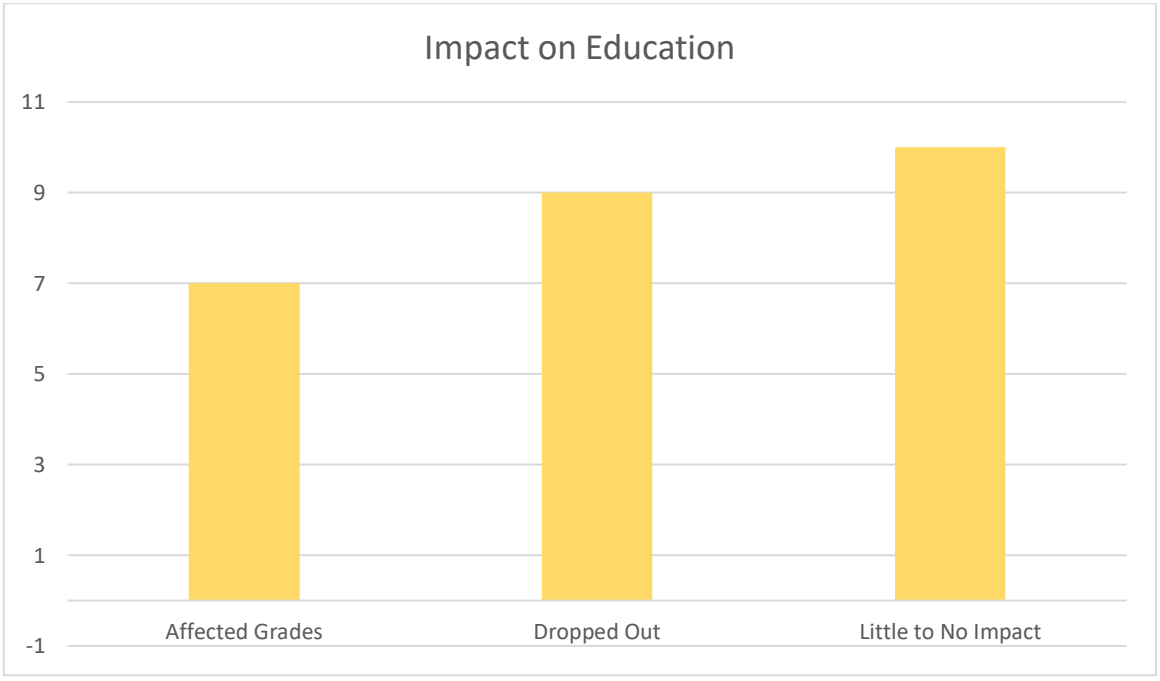

Figure 8. Effect on Education

4.5.8 Physical Effects

Out of 30 students who participated in the study, 23 were asked about any physical effects encountered due to the cyber fraud. Among these 23 students, eight were affected, resulting in a physical effect percentage of 35% (rounded to the nearest whole number), as presented in Table 7. The remaining 15 students confirmed that the cyber fraud incident had no indirect physical consequences for them.

Among the eight affected students, seven stated that they suffered from headaches due to the cyber fraud incident. Some resorted to medication for pain relief. Participant SABCF_021 expressed: "*I was so stressed; I would sometimes have a headache. So, I would go to buy pills that would assist with concentration*". Similarly, Participant SABCF_024 disclosed that the financial strain experienced during that period led to a reliance on medication, stating: "*I had tons and tons of headaches. And painkillers level two was my best friend*". Participant SABCF_028 shared a similar experience, saying: "*I sometimes have this terrible headache into my neck. I guess it was stress by that time. Most of the time I was drinking headache*

pills". Another student, participant SABCF_019, also resorted to medication due to the cyber fraud incident, explaining: "*At the time I used to buy me pills. Pills for my anxiety. Because I had palpitations at that time, heart palpitation, like my heart used to skip a beat. They used to help me a lot*". Lastly, Participant SABCF_017 noted that, in addition to headaches, they also experienced weight loss because of the cyber fraud incident.

Table 7. Effect of Cyber Fraud

Effect of Fraud	Number	Percentage
Financial loss	30	100%
Emotional	28	93%
Psychological	28	93%
Behavioural	30	100%
Education	16	61%
Physical	8	35%

4.6 Chapter Summary

In this chapter, the results of a qualitative analysis were presented based on research conducted on a diverse group of respondents. The respondents in this research varied in terms of education, gender, financial losses, and age. The age range of the participants ranged from 18 to 34 years old, with an average age of 23. The highest reported level of education ranged from NQF level 2 to NQF level 6, and most participants had non-English as their first language. All participants had experienced cyber fraud and incurred financial losses. The chapter explored the respondents' understanding of cyber fraud, revealing that 83% could define or explain "cyber fraud" or "online fraud". However, 90% of the respondents lacked formal training in cyber fraud. The chapter further explored the circumstances surrounding the cyber fraud incidents, including the events leading up to the fraud, the financial losses incurred, the support and assistance the victims received, and the time and out-of-pocket expenses related to the cyber fraud. Lastly, the chapter addressed the effect of cyber fraud on the students who were part of the study. It highlighted the consequences and aftermath of these cyber fraud experiences on the respondents.

In the next chapter, a discussion of these findings will be presented, providing a deeper analysis and interpretation of the results obtained in this qualitative study.

CHAPTER FIVE

5. DISCUSSION

5.1 Introduction

In the preceding chapters, we defined the research questions and objectives, introduced the research design, and presented the findings analyses. This chapter serves to connect the findings with the research questions. It includes a comprehensive discussion of the research findings and their alignment with the objectives. Students affected by cyber fraud shared their responses about their experiences and its effects. These responses offer insights into how institutions can better comprehend the effect of cyber fraud on students and provide the necessary support to mitigate its effect.

The rest of this chapter is organised as follows: Section 5.2 delves into the findings concerning the research objectives and relevant existing literature. Finally, Section 5.3 provides a summary of this chapter.

5.2 Discussion

The first research question that the researcher wanted to answer was: *What are South African higher education financial aid students' perceptions regarding cyber fraud?* The study found that 83% of participants understood or could explain the meaning of cyber fraud or online fraud, although most of them (90%) had no formal or informal training on the topic. This is consistent with Zarębska et al. (2023) findings who discovered that 76.5% of surveyed students knew others who had been victims of fraud, even though many of them had not experienced it themselves. Participant SABCF_024 experienced cyber fraud during her first year of receiving financial aid. The data suggests that most students lack the knowledge and skills to identify and protect themselves against fraudulent activities. These findings are also reported by Alharbi and Tassaddiq (2021), Xuezhou Zhang et al. (2022), Khamzina et al. (2022) and Zarębska et al. (2023).

The study found that 17% of participants stated that they did not practice safe online hygiene on their devices and took minimal or no precautions to safeguard themselves against online security threats. A study by Alqahtani (2022) found that university students lack cybersecurity awareness, particularly regarding password and account protection. Similarly, while applying for financial aid, several students sought assistance from strangers in completing their application, inadvertently exposing their personal information and possible login credentials. Many students realised they were victims of fraud when they could no longer access their

accounts. Others realised they were victims when they received notification that their account had been accessed and their contact details had been changed; some got a block status on their account when they tried to access their funds, and others found their accounts empty after logging on to the portal.

The events or circumstances that led to the cyber fraud varied amongst respondents, with many being social engineered by fake look-alike websites or disclosing their login details in exchange for assistance. It is worth noting that three students suspected the involvement of individuals within the student support office at the college, but these allegations lack evidence and warrant further investigation. Furthermore, two students believed someone close to them might be responsible for the cyber fraud they experienced, highlighting the importance of not sharing login credentials or using easily guessable passwords. When reporting the cyber fraud incidents, many students faced challenges, with some eventually giving up. Du Toit et al. (2018) identified a lack of awareness about cybercrime reporting procedures as the primary obstacle hindering individuals from reporting cybercrimes. Resolving account takeovers often took at least one week, with some cases extending to months or even years.

The second research question was: "*How are South African higher education financial aid students affected by cyber fraud"*? All participants in this study experienced financial losses. Modic and Anderson's (2015) study on internet fraud found that the extent of their financial losses significantly influences participants' emotional responses. Moreover, the severity of these emotional reactions is contingent upon the individual's wealth. As students were already in financially vulnerable positions, and none of the stolen money was returned, this direct financial effect was classified as high. It is essential to acknowledge that this research may not represent all victims, as it is biased towards reporting victims and primarily focuses on victims who reported the incidents. Only students who reported the fraud to the NSFAS were interviewed, excluding those who did not report the cyber fraud for various reasons such as difficulties contacting the call centre or not having airtime to contact the fraud hotline. Secondary effects of cyber fraud were also identified, including loss of time spent attempting to report and resolve the fraud, as well as additional expenses incurred for travelling to institutions or police stations and purchasing data or airtime.

While one student regained access to their account within a week, others required significantly more time, ranging from weeks to months and sometimes even years. Some individuals gave up trying. Consequently, the severity of this secondary effect is categorised as substantial. The direct financial and secondary effects of cyber fraud align with the findings of previous research in this field (Button, 2017; Jansen van Rensburg, 2018; Notté et al., 2021).

All interview participants exhibited noticeable behavioural changes following the cyber fraud incident. Most participants reported an increased sense of vigilance, particularly in their interactions on social media, phone calls, suspicious URLs, and the sharing of personal information. Some participants took proactive measures to alert others about potential online scams. Consequently, we can conclude that cyber fraud significantly influences the behaviour of its victims. This heightened awareness aligns with findings from studies conducted by Button (2017), Button et al. (2014), Jansen and Leukfeldt (2017), and Spalek (1999).

Interestingly, 17% of participants did not take specific actions to secure their devices against online security threats, as the fraud incident they experienced did not stem from vulnerabilities in their devices, such as malware. However, they did modify their online behaviour regarding links and sharing personal information. This change suggests that participants are now more cautious to prevent a recurrence of the same type of cyber fraud, as similarly noted by Drew (2020b).

Regarding the emotional and psychological consequences of cyber fraud, nearly all participants experienced the effect, with stress and anger being the most prevalent emotions. Other emotional effects included anxiety, anguish, sorrow, sadness, hopelessness, and depression. The psychological effect was characterised by 90% of participants losing trust in people, institutions, the government, or online platforms and 78% blaming themselves for the incident. These emotional and psychological consequences align with existing literature (Button, 2017; Jansen & Leukfeldt, 2017; Notté et al., 2021; Spalek, 1999), indicating that cyber fraud's emotional and psychological effect is significant. The physical effect was less common among participants, with only 35% reporting indirect physical effects such as headaches and some requiring medication. One student experienced sleep difficulty due to anxiety, while another had heart palpitations. These results are similar to the findings of Cross et al. (2016) and Jansen and Leukfeldt (2017) findings.

Among the participants, 62% reported an effect on their education, with 27% confirming that it affected their grades and 35% dropping out of their courses. Consistent with MMapatji (2023) findings, a lack of NSFAS allowances can negatively affect students' academic performance and motivation. This dropout rate is substantial, and the 38% who completed their studies attributed their success to factors such as emotional support, stable financial support, minimal financial losses from the fraud, and a strong determination to succeed despite the challenges. Notably, those who received emotional or financial support had a significantly lesser effect on their academic performance, compared to those who lacked support. This underscores the importance of support for victims of cyber fraud and its positive effects, as highlighted by Cross et al. (2016). For example, Participant SABCF_009, who regained access to their account and received financial assistance from friends and family, managed to pass despite the stress of

the fraud incident affecting her grades. Similarly, Participant SABCF_027 received financial support from their mother during the two months it took to regain access to their account. Unfortunately, their academic performance was affected by the cyber fraud incident due to missed classes.

Students who received assistance from NSFAS in regaining access to their accounts felt it helped them pass, as articulated by SABCF_027: "*Getting assistance was the end of my problems*". This underscores the significance of institutional support with a particular focus on the role played by NSFAS in aiding students to recover accounts that cybercriminals have compromised. It highlights how essential support is when considering the ramifications of cyber fraud on students receiving financial assistance. Additionally, the study identified a theme of student resilience and a determination to succeed in a handful of students, which was not considered a significant factor.

5.2.1 Practical Implications for Higher Education Institutions

This high percentage of students who had no formal or informal training on cyber security highlights the importance of cyber security awareness training for students, especially students receiving financial aid for the first time (Alharbi & Tassaddiq, 2021; Khamzina et al., 2022; Zarębska et al., 2023). Ezeji et al. (2018) emphasised the pivotal role of awareness in combating online crimes and underscored the necessity for collaboration between private and public institutions. Social engineering attacks are one of the more challenging attack vectors for students to recognise (Pósa & Grossklags, 2022), and fraud awareness training is a mechanism which can be used as a countermeasure (Button, 2017; Pósa & Grossklags, 2022). Leukfeldt and Yar (2016) state that heightened online risk awareness reduces susceptibility to victimisation. Student support services such as the financial aid assistants at institutions were also identified as a source of fraud and, Mabunda (2023) calls for these centres to refrain from requesting students' login details to prevent identity fraud. The implication is that these support centres are also in need of cyber security awareness training.

5.2.2 Practical Implications for NSFAS and policymakers

The researcher found that students were directed to a fraud hotline when contacting the NSFAS contact centre. Notably, the fraud hotline number is not zero-rated as purported by NSFAS, making it difficult for students to report the fraud due to limited airtime, which further delayed the process for affected victims. NSFAS should ensure that the fraud hotline provides comprehensive guidance to students when reporting cyber fraud to the police, considering that students required additional information during the reporting process. Furthermore,

resolving cases of students affected by cyber fraud should be a priority for NSFAS to minimise losses and expedite regaining account access (ACFE, 2022).

To protect financial aid recipients against cyber fraud, it is recommended that students undergo initial training and complete a cyber fraud aptitude assessment before their allowances are disbursed. The literature above underscores the importance of support for victims of cyber fraud and its positive effects. NSFAS could consider offering counselling programs for students affected by cyber fraud. NSFAS could consider collaborating with higher education institutions, many of which have counselling officers available to assist students. Furthermore, resolving cases of students affected by cyber fraud should be a priority for NSFAS to minimise losses and expedite regaining account access. NSFAS could consider establishing a student advisory committee composed of student champions or subject matter experts (SMEs) to offer support to students dealing with fraud-related issues, address application inquiries, raise awareness about emerging threats affecting students, and serve as a communication bridge between NSFAS administrators and student beneficiaries. The data analysis revealed instances where students proactively warned their peers about encountered scams, and the creation of such a student advisory body would be mutually advantageous for both NSFAS and its student beneficiaries. Additionally, NSFAS could implement robust password policies, as some students have reported that their passwords were easily guessable, often using only their birthdate as a password to access their allowance portal.

Most students expressed dissatisfaction with the level of assistance provided by the institutions. While one student reported the cyber fraud to the police station with relative ease, others found it daunting. A few participants expressed scepticism about the effectiveness of reporting to the police as they believed nothing would come from it. Notably, all cases reported by participants to the police remained unresolved, and no arrests were made. The police should take cyber fraud cases more seriously, as breakthroughs and arrests remain non-existent. Despite the presence of regulatory frameworks such as Section 8 of the Cybercrimes Act of 2020 (Act No. 19 of 2020) aimed at safeguarding the population against cyber fraud, it is argued that there exists a shortage of cybercrime expertise within law enforcement to effectively respond and combat these crimes (Dlamini & Mbambo, 2019; Ezeji et al., 2018). Law enforcement agencies and the prosecuting authority do not have the resources and manpower to tackle the growing epidemic of cyber fraud in South Africa (Mabunda, 2023). Ezeji et al. (2018) recommend that South African police officials at all levels should acquire fundamental skills in addressing cyber-related crimes, including identifying, categorising, and opening dockets for cybercrimes.

In summary, the findings have shown that there is a lack of communication between the three key stakeholders who are important in providing support to students: the police services, institution support and NSFAS. Each stakeholder presents attempts at addressing cyber fraud. For example, NSFAS through its website 'proactively communicates to students to always practice safe internet browsing/ online safety' and further outlines steps on how students can keep their accounts safe (https://www.nsfas.org.za/content/preventfraud.html). The police department also outlines a series of steps to follow to report an online crime in South Africa (ISPA, 2022), together with the National Cybersecurity Hub (South African National CSIRT, 2016). The goal of the Cybersecurity Hub is to work with stakeholders from government, the private sector, civil society and the public to make cyberspace a safe environment for communicating, socializing, and transacting. Despite these efforts, cyber fraud continues, with key targets, in the context of this study, being students and recently, NSFAS itself, whereby 'cyber criminals tried to gain unauthorised access to its payment infrastructure and that of its fintech partners' (Malinga, 2023). These findings suggest the need for policing, education institutions and NSFAS to actively pursue collaborative relationships amongst themselves and with other cyber fraud institutions such as the Cybersecurity Hub to curb cyber-related threats.

5.3 Chapter Summary

In this chapter, the results of a qualitative analysis were discussed. The study found that many participants understood or could explain the meaning of cyber fraud or online fraud, although the majority had no formal or informal training on the topic. The chapter further discussed the effect of cyber fraud on South African financial aid students, highlighting how such incidents can trigger a chain of adverse consequences which could ultimately affect a student's education, particularly in the absence of support. These consequences encompass financial, psychological, emotional, behavioural, and secondary effects.

The next chapter presents a conclusion and recommendations that summarize the key findings, address limitations, and suggest areas for future research.

CHAPTER SIX

6. CONCLUSION

6.1 Introduction

The goal of this study was to identify and understand how South African higher education financial aid students perceive cyber fraud; and how cyber fraud affects them. The previous chapter discussed the results of the qualitative analysis of students' perceptions of cyber fraud and its effect on South African financial aid students. Chapter 1 introduced the study, including a discussion of the research problem, research questions and objectives, and rationale for the study. Chapter 2 presents a literature review on prior research related to cyber fraud, along with an overview of the NSFAS. Chapter 3 presented the methodology employed for data collection and analysis in this study, and Chapter 4 delves into a thorough examination of data analysis and findings.

This chapter presents a summary, highlights key findings, offers recommendations, acknowledges limitations, and suggests directions for future research.

6.2 Summary

Financial aid is critical to enable higher education for many poor students in South Africa (Garrod & Wildschut, 2021; Wildschut-February et al., 2018), and it is crucial to understand the effect of cyber fraud on these students. Understanding these effects is essential because the people affected by cyber fraud are often the ones in vulnerable positions (IPSFF, 2020). South African higher education financial aid students are one of these vulnerable groups as they come from poor backgrounds. Financial aid recipients are particularly susceptible to cyber fraud, given their reliance on financial services and potentially limited financial resources to mitigate losses. Cyber fraud does not only have a financial loss effect, but it can also have devastating effects on an individual's well-being, which can include issues relating to health, relationships, and self-harm (Button & Cross, 2017).

This study had three key objectives: first, to understand how South African higher education financial aid students perceive cyber fraud; second, to identify the perceived events that led to cyber fraud; and third, to identify the effects of cyber fraud on the victims. The study adopted a qualitative enquiry approach and employed purposive and snowball sampling techniques to select participants for the National Student Financial Aid Scheme. Data was collected using

semi-structured interviews with 30 beneficiaries of the scheme, all of whom had experienced cyber fraud. Thematic analysis was applied to analyse the gathered data.

The findings show that most students were aware of cyber fraud and understood it to be a type of fraud committed by individuals using technology for monetary or information gains. The awareness and understanding were not gained through formal education but rather from events they experienced firsthand or observed others experiencing. The lack of formalised awareness and training on cyber fraud for vulnerable communities has increased their risk of becoming victims, thereby placing them in more vulnerable positions than before. This study identified four sources of events that led to cyber fraud: social engineering, the use of online application portals for NSFAS funding, the use of institutional support services, and assistance from family, friends and acquittances. Although most victims could discuss the incident with their families and friends, most noted minimal support from the institutions they approached, namely the police, NSFAS and their respective institutions where they were registered for their studies. This study recommends that institutional (policing, education institutions and NSFAS) and social support structures be put in place for vulnerable communities to curb the sources of these events.

Financial aid students affected by cyber fraud come from diverse backgrounds and possess different characteristics. There is no one "type" of person vulnerable to cyber fraud. The study found that some victims coped better than others, with those having financial or emotional support recovering more easily. The researcher agrees with Button et al. (2014) that online financial fraud is not a victimless crime, as the effect on students can be devastating. Institutions such as colleges, the police, and NSFAS should display greater empathy in dealing with students affected by cyber fraud as they play a vital role in helping victims recover from the effects. The most cited effects of cyber fraud on students were financial loss and emotional effects. This was followed by psychological effects that resulted in self-blame, lack of trust in people, institutions, and online communities. The effects resulted in noticeable behavioural changes in the victim’s actions, with most reporting an increased sense of vigilance and becoming suspicious in their interactions; as well as taking proactive measures to alert others about potential online scams. These findings are encouraging, and the study reemphasises the need for structural support and understanding of why fraud victims continue to bear the blame and are not given the required support.

The findings in this study contributes to the broader discussion of cyber security by highlighting the need to focus on the higher education sector and the social support systems available for use by all stakeholders, particularly students from vulnerable backgrounds. Studies on cyber security tend to focus primarily on other sectors, particularly the private sector with large

organizations. The higher education sector receives limited attention, particularly HEI in the emerging economies of Africa where cyber-attacks are perceived to be widespread. Most scholars on cyber security have tended to follow a more technical approach to address the IT security systems in place, which in the NSFAS context, are perceived as still 'not up to scratch' (Ndenze, 2024). Although this is warranted, this approach fails to zoom into the context-specific nuances such as how cyber incidents affect the most vulnerable in society. By not addressing the socio-implications of cyber security incidents, the proportionality of these attacks and consequences on human life and organizations alike will be catastrophic.

6.3 Limitations and Future Work

This study acknowledges certain limitations. The sample selection process introduced a bias towards reporting victims, as only those who reported the fraud to NSFAS were interviewed. Consequently, the study does not provide insights into the effect of cyber fraud on non-reporting victims. Furthermore, the generalizability of the findings is restricted to financially vulnerable financial aid students and may not extend to all bursary recipients affected by cyber fraud. It is also important to note that this study relied on self-reported data. Although telephone interviews offered convenience for both the researcher and participants, in-person interviews would have been better suited for this type of research due to the sensitive nature of the topic and the participants' experiences with cyber fraud. Some participants exhibited reluctance to disclose specific information regarding the effect of cyber fraud on them, which is attributable to a lack of trust in the interviewer. Given the participants' heightened distrust and scepticism because of the cyber fraud, they experienced, in-person interactions would have facilitated personal connection, fostered rapport, and enhanced trust-building, leading to more comprehensive and insightful data collection.

Future studies could investigate the effect of cyber fraud on bursary recipients or non-bursary recipients who are less financially vulnerable. Additionally, longitudinal studies could investigate the long-term effects of cyber fraud on victims, focusing on their coping mechanisms, financial struggles, and challenges in rebuilding trust. Future research projects could also determine the most effective methods for delivering training and awareness programs to assist financial aid students in safeguarding themselves against cyber fraud.

7. REFERENCES

Abdulai, M. A. (2020). Examining the effect of victimization experience on fear of cybercrime: University students' experience of credit/debit card fraud. *International Journal of Cyber Criminology*, *14*(1), 157–174. https://doi.org/10.5281/zenodo.3749468

ACFE. (2022). *Occupational Fraud 2022: A Report to the nations* (12). http://www.acfe.com/report-to-the-nations/2022/

Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., & Upton, D. (2018). A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, *4*(1). https://doi.org/10.1093/cybsec/tyy006

Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: A cross sectional study. *Crime Science*, *13*(1), 29. https://doi.org/10.1186/s40163-024-00230-w

Ajoy, P. B. (2022). Effectiveness of criminal law in tackling cybercrime: A critical analysis. *Sch Int J Law Crime Justice*, *5*(2). https://doi.org/10.36348/sijlcj.2022.v05i02.005

Alharbi, T., & Tassaddiq, A. (2021). Assessment of Cybersecurity Awareness among Students of Majmaah University. *Big Data and Cognitive Computing*, *5*(2). https://doi.org/10.3390/bdcc5020023

Ali, M. M., & Mohd Zaharon, N. F. (2022). Phishing—A Cyber Fraud: The Types, Implications and Governance. *International Journal of Educational Reform*, *11*(1). https://doi.org/10.1177/10567879221082966

Alqahtani, M. A. (2022). Factors Affecting Cybersecurity Awareness among University Students. *Applied Sciences*, *12*(5). https://doi.org/10.3390/app12052589

Al-Saadi, H. (2014). *Demystifying ontology and epistemology in research methods*. *Research gate 1(1)*, 1–10. https://www.researchgate.net/publication/260244813_Demystifying_Ontology_and_Epistemology_in_Research_Methods#:~:text=Two%20epistemological%20assumptions%20are%20referred,Al%2DSaadi%2C%202014)%20.

Aphane, M. P. (2023). Cybersecurity Awareness on Cybercrime Among the Youth in Gauteng Province. *International Journal of Social Science Research and Review*, *6*(8), 23–32. https://doi.org/10.47814/ijssrr.v6i8.1414

Arthur, W. B. (1994). Inductive reasoning and bounded rationality. *The American economic review*, *84*(2), 406-411.

Awang, N., Hussin, N. S., Razali, F., & Abu Talib, S. (2021). Fraud Triangle Theory: Calling for New Factors. *Insight Journal*, *7*, 54–64. https://doi.org/10.24191/ij.v7i0.87

Babbie, E., Beiting-Lipps, E., & Kindstrom, K. (2015). *The practice of social research* (14th ed.). Cengage Learning. http://ebookcentral.proquest.com/lib/uoct/detail.action?docID=4332975

Baker, M. (2020). Feds suspect vast fraud network is targeting US unemployment systems. *The New York Times*.

Bhattacherjee, A. (2012). *Social science research: Principles, methods, and practices*. https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=1002&context=oa_textbooks

Bhengu, C. (2021, October 28). *Here's how scammers may gain access to your NSFAS allowance*. https://bit.ly/3pICHNm

Bitzer, E., & Jager, E. D. (2018). The views of commerce students regarding "free" higher education in South Africa. *South African Journal of Higher Education*, *32*(4). https://doi.org/10.20853/32-4-2436

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2). https://doi.org/10.1191/1478088706qp063oa

Bryman, A., & Bell, E. (2011). *Business research methods* (3rd ed). Oxford University Press. https://www.uwcentre.ac.cn/haut/wp-content/uploads/2018/11/Alan_Bryman_Emma_Bell_Business_Research_Methodsb-ok.cc.pdf

Burrell, G., & Morgan, G. (1979). *Sociological paradigms and organisational analysis: Elements of the sociology of corporate Life*. Routledge. https://doi.org/10.4324/9781315242804

Button, M. (2017). *Cyber frauds, scams and their victims.* (1st ed.). Taylor and Francis. https://doi.org/10.4324/9781315679877

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021a). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. *Telematics and Informatics*, *64*, 101675. https://doi.org/10.1016/j.tele.2021.101675

Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021b). Victims of Cybercrime: Understanding the Impact Through Accounts. In M. Weulen Kranenbarg & R. Leukfeldt (Eds.), *Cybercrime in Context: The human factor in victimization, offending, and policing* (pp. 137–156). Springer International Publishing. https://doi.org/10.1007/978-3-030-60527-8_9

Button, M., & Cross, C. (2017). *Not a victimless crime: The impact of fraud upon victims* (1st ed., pp. 91–114). Routledge. https://doi.org/10.4324/9781315679877-4

Button, M., Lewis, C., & Tapley, J. (2009). *Fraud typologies and the victims of fraud: Literature review* (p. 40). National Fraud Authority. https://researchportal.port.ac.uk/en/publications/fraud-typologies-and-the-victims-of-fraud-literature-review

Button, M., Lewis, C., & Tapley, J. (2014). Not a victimless crime: The impact of fraud on individual victims and their families. *Security Journal*, *27*(1), 36–54. https://doi.org/10.1057/sj.2012.11

C3SA, C. C. C. for S. A. (2022). *Southern African Development Community Cybersecurity Maturity Report 2021*. OpenUCT. http://hdl.handle.net/11427/36211

Chigada, J., & Madzinga, R. (2021). Cyberattacks and threats during COVID-19: A systematic literature review. *SA Journal of Information Management*, *23*(1). https://doi.org/10.4102/sajim.v23i1.1277

Cooper, D. R., & Schindler, P. S. (2014). *Business Research Methods* (4th ed.). McGraw-Hill. https://www.worldcat.org/title/business-research-methods/oclc/879166049

Cressey, D. R. (1953). *Other people's money; a study of the social psychology of embezzlement.* (p. 191). Free Press. https://doi.org/10.1086/221475

Creswell, J. W. (2013). *Research design: Qualitative, quantitative, and mixed methods approaches* (4th ed.). SAGE. https://books.google.co.za/books/about/Research_Design.html?id=PViMtOnJ1LcC&redir_esc=y

Cross, C. (2019). Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice*, *5*. https://doi.org/10.1108/JCRPP-01-2019-0008

Cross, C., & Holt, T. J. (2021). The use of military profiles in romance fraud schemes. *Victims & Offenders*, *16*(3). https://doi.org/10.1080/15564886.2020.1850582

Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice [Electronic Resource]*, *518*, 1–14. https://search.informit.org/doi/10.3316/informit.300566903591621

DHET. (2007). *The Higher Education Qualifications Framework HIGHER EDUCATION ACT, 1997 (Act No. 101 of 1997)*. Department of Education. https://www.dhet.gov.za/Policy%20and%20Development%20Support/The%20High%20Education%20Qualifications%20Framework%20(HEQF).pdf

DHET. (2021). *Minister Blade Nzimande: NSFAS 2022 applications official opening | South African Government*. Minister Blade Nzimande: NSFAS 2022 Applications Official Opening. https://www.gov.za/speeches/minister-blade-nzimande-nsfas-2022-applications-official-opening-28-oct-2021-0000

Dlamini, S., & Mbambo, C. (2019). Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses. *Cogent Social Sciences*, *5*(1), 1675404. https://doi.org/10.1080/23311886.2019.1675404

Drew, J. M. (2020). A study of cybercrime victimisation and prevention: Exploring the use of online crime prevention behaviours and strategies. *Journal of Criminological Research, Policy and Practice*, *6*(1). https://doi.org/10.1108/JCRPP-12-2019-0070

Du Toit, R., Hadebe, P. N., & Mphatheni, M. (2018). Public perceptions of Cybersecurity: A South African context. *Acta Criminologica: African Journal of Criminology & Victimology*, *31*(3), 111–131. https://hdl.handle.net/10520/EJC-14d9e12e41

Ezeji, C. L., Olutola, A. A., & Bello, P. O. (2018). Cyber-related crime in South Africa: Extent and perspectives of state's roleplayers. *Acta Criminologica : African Journal of Criminology & Victimology*, *31*(3), 93–110. https://doi.org/10.10520/EJC-14d9dc60ec

Garrod, N., & Wildschut, A. (2021). How large is the missing middle and what would it cost to fund? *Development Southern Africa*, *38*(3). https://doi.org/10.1080/0376835X.2020.1796594

Government Gazette. (2021). *Act No. 19 of 2020: Cybercrimes Act, 2020*. Act No. 19 of 2020: Cybercrimes Act, 2020. https://www.gov.za/sites/default/files/gcis_document/202106/44651gon324.pdf

Guba, E. G., & Lincoln, Y. S. (1982). Epistemological and Methodological Bases of Naturalistic Inquiry. *Educational Communication and Technology*, *30*(4). JSTOR. https://doi.org/10.1007/BF02765185

Hidayati, A. N., Riadi, I., Ramadhani, E., & Al Amany, S. U. (2021). Development of conceptual framework for cyber fraud investigation. *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, *7*(2). https://doi.org/10.26594/register.v7i2.2263

Hlongwane, N. W., & Daw, O. D. (2021). UNEMPLOYMENT AND ECONOMIC GROWTH IN SOUTH AFRICA FROM 1980 TO 2020 AN ARDL APPROACH. *International Journal of Economics and Finance Studies*, *13*(2).

Ho, H. T. N., & Luong, H. T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. *SN Social Sciences*, *2*(1). https://doi.org/10.1007/s43545-021-00305-4

Holstein, J. A., & Gubrium, J. F. (1995). *The Active Interview*. SAGE Publications. https://books.google.co.ls/books?id=LgR3TjzCxf8C

Holt, A. (2010). Using the telephone for narrative interviewing: A research note. *Qualitative Research*, *10*(1), 113–121. https://doi.org/10.1177/1468794109348686

Hudson, L. A., & Ozanne, J. L. (1988). Alternative ways of seeking knowledge in consumer research. *Journal of Consumer Research*, *14*(4). https://doi.org/10.1086/209132

Hussin, N., & Zawawi, M. (2012). Preventing criminal victimization through community education: An Islamic formula. *Procedia - Social and Behavioral Sciences*, *68*, 855–864. https://doi.org/10.1016/j.sbspro.2012.12.272

Hutchinson, G., & Ophoff, J. (2020). *A Descriptive Review and Classification of Organizational Information Security Awareness Research* (Vol. 1166, pp. 114–130). Springer International Publishing. https://doi.org/10.1007/978-3-030-43276-8_9

IPSFF. (2020). *Guide to Understanding the Total Impact of Fraud* [Government]. Guide to Understanding the Total Impact of Fraud. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/866608/2377_The_Impact_of_Fraud_AW__4_.pdf

ISPA, 2022. *Reporting cybercrimes*. https://ispa.org.za/wp-content/uploads/2022/10/ISPA-Advisory-Reporting-Cybercrimes-Updated-October-2022.pdf

Jansen, J., & Leukfeldt, R. (2017). Coping with Cybercrime Victimization: An Exploratory Study into the Impact and Change. *Journal of Qualitative Criminal Justice & Criminology*. https://doi.org/10.21428/88de04a1.976bcaf6

Jansen van Rensburg, S. (2018). Contextualising social engineering through criminological theorising. *Acta Criminologica : African Journal of Criminology & Victimology*, *31*(3). https://doi.org/10.10520/EJC-14d8ef57a9

Kemp, S. (2022). Fraud reporting in Catalonia in the Internet era: Determinants and motives. *European Journal of Criminology*, *19*(5), 994–1015. https://doi.org/10.1177/1477370820941405

Kemp, S., Miró-Llinares, F., & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*, *26*(3). https://doi.org/10.1007/s10610-020-09439-2

Khamzina, B., Roza, N., Zhussupbekova, G., Shaizhanova, K., Aten, A., & Aigerim Meirkhanovna, B. (2022). Determination of Cyber Security Issues and Awareness Training for University Students. *International Journal of Emerging Technologies in Learning (iJET)*, *17*(18), 177–190. https://doi.org/10.3991/ijet.v17i18.32193

Kimpe, L., Walrave, M., & Ponnet, K. (2020). *The human face of cybercrime. Identifying targets, victims, and their coping mechanisms*. https://books.google.co.za/books?id=OLPgzQEACAAJ

King, J., & Doig, A. (2016). A dedicated place for volume fraud within the current UK economic crime agenda?: The Greater Manchester police case study. *Journal of Financial Crime*, *23*, 902–915. https://doi.org/10.1108/JFC-07-2015-0036

Knüpfer, S., Rantala, V., & Vokata, P. (2021). Scammed and scarred: Effects of investment fraud on its victims. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3850928

Lazarus, S., Button, M., & Kapend, R. (2022). Exploring the value of feminist theory in understanding digital crimes: Gender and cybercrime types. *The Howard Journal of Crime and Justice*, *61*(3), 381–398. https://doi.org/10.1111/hojo.12485

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Levi, M., Doig, A., Gundur, R. V., Wall, D., & Williams, M. (2015). *The Implications of Economic Cybercrime for Policing*. https://doi.org/10.13140/RG.2.1.3357.2566

Lewins, A., & Silver, C. (2009). *Choosing a CAQDAS Package* [Working Paper]. University of Surrey. http://caqdas.soc.surrey.ac.uk/PDF/2009ChoosingaCAQDASPackage.pdf

Ma, K. W. F., & McKinnon, T. (2022). COVID-19 and cyber fraud: Emerging threats during the pandemic. *Journal of Financial Crime*, *29*(2). https://doi.org/10.1108/JFC-01-2021-0016

Mabunda, S. (2023). IS IT CYBERFRAUD OR GOOD OL' OFFLINE FRAUD? A LOOK AT SECTION 8 OF THE SOUTH AFRICAN CYBERCRIMES BILL. *Journal of Anti-Corruption Law*, *2*. https://doi.org/10.14426/jacl.v2i1.1283

Mabuza, N. H. (2020). *Dropout causes of students funded by the National Student Financial Aid Scheme in South African universities* [Thesis]. https://uir.unisa.ac.za/handle/10500/26730

Malinga S., 2023. *NSFAS beefs up IT security to protect students' funds*. https://www.itweb.co.za/article/nsfas-beefs-up-it-security-to-protect-students-funds/Pero3MZ3epRqQb6m

Mashale, K. (2023). Students bust for siphoning friend's NSFAS funds. *Sowetanlive*. https://www.sowetanlive.co.za/news/south-africa/2023-07-24-students-bust-for-siphoning-friends-nsfas-funds/

Mashale K. (2023). Students need to be vigilant when using payment platforms, NSFAS warns. Retrieved from https://www.sowetanlive.co.za/news/south-africa/2023-08-18-students-need-to-be-vigilant-when-using-payment-platforms-nsfas-warns/

Matlhabe G. (2023). NSFAS to probe attempts to steal student data amid cyberattacks. Retrieved from https://www.iol.co.za/the-star/news/nsfas-to-probe-attempts-to-steal-student-data-amid-cyberattacks-a4d277bd-3012-4d81-80ad-2de5b9085e1c

Mbovane, T. (2019). Students lay charges of fraud against NSFAS. *GroundUp*. https://www.groundup.org.za/article/port-elizabeth-students-open-cases-fraud-accuse-nsfas/

Mcguire, M., & Dowling, S. (2013). *Cyber crime: A review of the evidence*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf

MMapatji, T. B. (2023). *The impact of student protests on motivation, academic performance, and retention rate at Nkangala TVET college, Mpumalanga province* [UNISA]. https://hdl.handle.net/10500/30380

Modic, D., & Anderson, R. (2015). It's All Over but the Crying: The Emotional and Financial Impact of Internet Fraud. *IEEE Security & Privacy*, *13*(5), 99–103. https://doi.org/10.1109/MSP.2015.107

Myers, M. D. (1997). Qualitative Research in Information Systems. *MIS Quarterly*, *21*(2). https://doi.org/10.2307/249422

Mykhalchenko, N., & Wiegratz, J. (2019). Anti-fraud measures in Southern Africa. *Review of African Political Economy*, *46*(161). https://doi.org/10.1080/03056244.2019.1660156

Naidoo, R. (2020). A multi-level influence model of COVID-19 themed cybercrime. *European Journal of Information Systems*, *29*(3). https://doi.org/10.1080/0960085X.2020.1771222

Ndenze B. (2024). NSFAS says ICT system is still 'not up to scratch'. Retrieved from https://www.ewn.co.za/2024/08/21/nsfas-says-ict-system-is-still-not-up-to-scratch

Notté, R., Leukfeldt, E. R., & Malsch, M. (2021). Double, triple or quadruple hits? Exploring the impact of cybercrime on victims in the Netherlands. *International Review of Victimology*, *27*(3), 272–294. https://doi.org/10.1177/02697580211010692

NSFAS. (2021a). *National Student Financial Aid Scheme*. National Student Financial Aid Scheme. https://www.nsfas.org.za/content/faqs.html

NSFAS. (2021b). *National Student Financial Aid Scheme*. Fraud Prevention. https://www.nsfas.org.za/content/preventfraud.html

NSFAS. (2022). *NSFAS Annual Reports 2010—2021*. NSFAS Annual Reports. https://www.nsfas.org.za/content/annual-reports.html

NSFAS. (2023). *Fraud Prevention*. Fraud Prevention. https://www.nsfas.org.za/content/preventfraud.html

Ochoa Hernandez, R., Simpson, A., & Gill, G. (2021). *The human impacts of fraud*. Macquarie University. https://doi.org/10.25949/1Y9X-X522

Odeku, K. O. (2021). Socio-economic implications of covid-19 pandemic in South Africa. *Academy of Entrepreneurship Journal*, *27*, 1–6.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying Information Technology in organizations: Research approaches and assumptions. *Information Systems Research*, *2*(1). JSTOR. https://doi.org/10.1287/isre.2.1.1

Patten, M. L., & Newhart, M. (2017). *Understanding research methods: An overview of the essentials*. Routledge. https://doi.org/10.4324/9781315213033

Pillay, N., Bhorat, H., & Asmal, Z. (2021). *Higher Education Outcomes in South Africa: The Role of the National Student Financial Aid Scheme* (pp. 171–194). https://doi.org/10.1007/978-3-030-65417-7_10

Pósa, T., & Grossklags, J. (2022). Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students. *Journal of Cybersecurity and Privacy*, *2*(3), 490–515. https://doi.org/10.3390/jcp2030025

Raj, A., Jain, N., & Chauhan, S. S. (2021). Mapping of Security Issues and Concerns in Cloud Computing with Compromised Security Attributes. In R. Agrawal, G. Sanyal, K. Curran, V. E. Balas, & M. S. Gaur (Eds.), *Cybersecurity in Emerging Digital Era* (pp. 24–40). Springer International Publishing. https://doi-org.ezproxy.uct.ac.za/10.1007/978-3-030-84842-2_2

Ratner, C. (2002). Subjectivity and Objectivity in Qualitative Methodology. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, *3*(3). https://doi.org/10.17169/fqs-3.3.829

Saeed, M., & Osakwe, S. (2021). *Are African countries doing enough to ensure cybersecurity and internet safety?* Africa Portal. https://policycommons.net/artifacts/1819250/are-african-countries-doing-enough-to-ensure-cybersecurity-and-internet-safety/2556712/

Samuels, S. (2021). *Scammers are on the hunt for NSFAS money again*. Scammers Are on the Hunt for NSFAS Money Again. https://www.careersportal.co.za/news/scammers-are-on-the-hunt-for-nsfas-money-again

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson. https://www.pearson.com/nl/en_NL/higher-education/subject-catalogue/business-and-management/Research-methods-for-business-students-8e-saunders.html

Siahaan, A. P. U., & Nasution, M. D. T. P. (2018). The Phenomenon of Cyber-Crime and Fraud Victimization in Online Shop. *INA-Rxiv*, Article juec4. https://ideas.repec.org//p/osf/inarxi/juec4.html

South African National CSIRT, 2016. The Cybersecurity Hub. https://www.cybersecurityhub.gov.za/

Spalek, B. (1999). Exploring the Impact of Financial Crime: A Study Looking into the Effects of the Maxwell Scandal upon the Maxwell Pensioners. *International Review of Victimology*, *6*(3). https://doi.org/10.1177/026975809900600304

Statistics South Africa. (2020). *Quarterly Labour Force Survey (QLFS) – Q4:2019 | Statistics South Africa*. https://www.statssa.gov.za/?p=12948

Statistics South Africa. (2022). *Quarterly Labour Force Survey (QLFS) – Q4:2021 | Statistics South Africa*.

http://www.statssa.gov.za/publications/P0211/Media%20release%20QLFS%20Q4%202021.pdf

Stevens, F., Nurse, J. R. C., & Arief, B. (2021). Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systematic Review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367–376. https://doi.org/10.1089/cyber.2020.0253

The IIA's. (2019). *Assurance Over Fraud Controls Fundamental to Success—FRAUD AND INTERNAL AUDIT*. The Institute of Internal Auditors. https://www.theiia.org/globalassets/documents/resources/fraud-and-internal-audit-assurance-over-fraud-controls-fundamental-to-success-april-2019/fraud-and-internal-audit.pdf

Thwala, H. (2022). DUT students duped in NSFAS allowances scam. *IOL*. https://www.iol.co.za/education/universities/dut-students-duped-in-nsfas-allowances-scam-e1069f25-4451-4a4a-b097-d7b6a55351d3

Trozze, A., Kamps, J., Akartuna, E. A., Hetzel, F. J., Kleinberg, B., Davies, T., & Johnson, S. D. (2022). Cryptocurrencies and future financial crime. *Crime Science*, *11*(1). https://doi.org/10.1186/s40163-021-00163-8

Vousinas, G. (2019). Advancing theory of fraud: The S.C.O.R.E. model. *Journal of Financial Crime*, *26*(1). https://doi.org/10.1108/JFC-12-2017-0128

Wakefield, H. I., Yu, D., & Swanepoel, C. (2022). Revisiting transitory and chronic unemployment in South Africa. *Development Southern Africa*, *39*(2). https://doi.org/10.1080/0376835X.2020.1799761

Whitty, M. T. (2019). Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime*, *26*(1). https://doi.org/10.1108/JFC-10-2017-0095

Whitty, M. T., & Buchanan, T. (2016). The online dating romance scam: The psychological impact on victims – both financial and non-financial. *Criminology & Criminal Justice*, *16*(2). https://doi.org/10.1177/1748895815603773

Wildschut-February, A., Mncwango, B., Rust, J., Fongwa, S., & Rogan, M. (2018). *The National Student Financial Aid Scheme (NSFAS) and its impact: Exploring the absorption into employment of NSFAS-funded graduates project team absorption into employment of NSFAS funded graduates study*. Human Sciences Research Council (HSRC). https://doi.org/10.13140/RG.2.2.30412.26242

Wira Utami, D. P., & Purnamasari, D. I. (2021). The impact of ethics and fraud pentagon theory on academic fraud behavior. *Journal of Business and Information Systems (e-ISSN: 2685-2543)*, *3*(1). https://doi.org/10.36067/jbis.v3i1.88

Xuezhou Zhang, Yan Qu, & Ting Zhu. (2022). An Empirical Study on the Current Situation of College Students' Financial Fraud and Its Influencing Factors. *Proceedings of the 2022 2nd International Conference on Business Administration and Data Science (BADS 2022)*, 624–632. https://doi.org/10.2991/978-94-6463-102-9_65

Zarębska, J., Howis, N., & Barska, M. (2023). Research on students' perception of information technology security – a new era of threats. *Scientific Papers of Silesian University of Technology. Organization and Management Series*, *2023*, 709–721. https://doi.org/10.29119/1641-3466.2023.170.43

8. APPENDIX

8.1 Appendix A – Cover Letter

Department of Information Systems

Leslie Commerce Building

Private Bag. Rondebosch 7701

Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280

Internet: http://www.commerce.uct.ac.za/informationsystems/

30 September 2022

Dear Sir/Madam,

I, Gershon Hutchinson am doing a research project under the supervision of Salah Kabanda, an Associate Professor in the Department of Information Systems towards a Master of Commerce degree at the University of Cape Town. We are inviting you to participate in a research study entitled the impact of cyber fraud on higher education financial aid students in South Africa.

The objective of this study is to understand how higher education financial aid students are affected by cyber fraud in South Africa. This research has been approved by the Commerce Faculty Ethics in Research Committee.

Your participation is important in enabling me to fully understand the topic at hand. Your decision to partake in this study is entirely voluntary. All information will be treated in a confidential manner and used exclusively for the purpose of this study. No individual names will be recorded or published. You will not be requested to supply any identifiable information, ensuring anonymity of your responses. You can choose to withdraw from this research study at any time.

The data collection method will be one-on-one interviews. The interview will take approximately 30 minutes. The findings of the research will be presented in a report to the University of Cape Town. The findings may also be published in an academic journal or in a conference paper. A copy of the report may be made available for all participants to examine.

There are no foreseeable risks for taking part in the study. If you are willing to participate in this study, kindly sign the attached consent form and return it to me at your earliest convenience.

Should you have any questions regarding this research, please feel free to contact me on 0672921962 or htcger001@myuct.ac.za

Your participation in this study would be greatly appreciated but is entirely voluntary.

Sincerely,

Gershon Hutchinson

Gershon Hutchinson

Masters Student

Department of Information Systems

University of Cape Town

Email: htcger001@myuct.ac.za

Salah Kabanda

Research Supervisor

Department of Information Systems

University of Cape Town

Email: salah.kabanda@uct.ac.za

8.2 Appendix B – Consent Form

Department of Information Systems

Leslie Commerce Building

Private Bag. Rondebosch 7701

Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280

Internet: http://www.commerce.uct.ac.za/informationsystems/

Research Participant Consent Form: Interviews

I, _____ (participant name), consent to participate in the research on the impact of cyber fraud on higher education financial aid students in South Africa.

I confirm that the researcher has informed me about the nature of the study, and I have had the opportunity to ask questions about the project.

I am aware that participation is voluntary and that I may choose to withdraw from this study at any time, without giving any reasons, and without there being any negative consequences, should I choose to do so.

I understand that should I not wish to answer any question or questions; I am free to decline.

I understand my responses and personal data will be kept strictly confidential. I understand that my name will not be linked with the research materials, and I will not be identified or identifiable in the reports or publications that result from the research.

I am aware that the findings of this study could be processed into a journal publication, research report, or conference proceedings, and my participation will be kept confidential.

I agree that the interview may be recorded.

_____	_____	_____
Name of Participant	Date	Signature

8.3 Appendix C – Letter to the NSFAS

Department of Information Systems

Leslie Commerce Building

Private Bag. Rondebosch 7701

Tel: +27 (0) 21 650 4028 Fax: +27 (0) 21650 2280

Internet: http://www.commerce.uct.ac.za/informationsystems/

30 September 2022

Request for information on financial aid students affected by cyber fraud

Dear Sir/Madam,

I, Gershon Hutchinson am doing a research project under the supervision of Salah Kabanda, an Associate Professor in the Department of Information Systems towards a Master of Commerce degree at the University of Cape Town. We are inviting you to participate in a research study entitled the impact of cyber fraud on higher education financial aid students in South Africa. This research has been approved by the University of Cape Town (UCT)'s Commerce Faculty Ethics in Research Committee. The researcher has set a target of 30 participants for this research study and would like to request your assistance with permission to acquire a list of financial aid students who had been affected by cyber fraud to participate in this study.

The objective of this study is to understand how higher education financial aid students are affected by cyber fraud in South Africa. Your participation is important in enabling me to fully understand the topic at hand.

Participation in this research is voluntary. All information will be treated in a confidential manner and used exclusively for the purpose of this study. No individual names will be recorded or published. Participants will not be requested to supply any identifiable information, ensuring anonymity of their responses. They can choose to withdraw from the research at any time for whatever reason, in accordance with ethical research requirements. The data collection method will be one-on-one interviews. The interview will take approximately 30 minutes. The findings of the research will be presented in a report to the University of Cape Town. The findings may also be published in an academic journal or in a conference paper. A copy of the report may be made available for all participants to examine.

Should you have any questions regarding this research, please feel free to contact me on 0672921962 or htcger001@myuct.ac.za.

Sincerely,

Gershon Hutchinson

Masters Student

Department of Information Systems

University of Cape Town

Email: htcger001@myuct.ac.za

Salah Kabanda

Research Supervisor

Department of Information Systems

University of Cape Town

Email: salah.kabanda@uct.ac.za

8.4 Appendix D – Application to Conduct Research

National Student Financial Aid Scheme

RE: APPLICATION TO CONDUCT RESEARCH: MR GERSHON HUTCHINSON - UCT

Mr Gershon Hutchinson
Leslie Commerce Building
Private Bag x3
Rondebosh
7701

Your application to conduct research study was received and acknowledged. The title of your research project reads: "The Impact of Cyber Fraud on Higher Education Financial Aid students in South Africa". I trust that the aims and the objectives of the study will benefit the organization and our beneficiaries. Your request is approved subject to you observing the provisions of the ethics clearance and the University of Cape Town's departmental research policy.

You are requested to share your findings with the relevant sections of the organization for review and consideration. We may also consider implementing any controls based on your findings if that will be in the best interests of the organization. To this effect, your final approved research report (both soft and hard copy) should be submitted to the organization. You may also be required to prepare a presentation and present it to the organization.

The organization wishes you well on your research project.

Mr. Modibedi Oliphant
Executive: Chief Information Officer

10 Brodie Road, House Vincent, 2nd Floor, Wynberg, Cape Town, 7700 | Private Bag X1, Plumstead, Cape Town, 7800
Tel No.: 0800 067 327 | 021 763 3200 | Email: info@nsfas.org.za

8.5 Appendix E – NVIVO Codebook

Name	Description	Files	References
Contextual Background	This code is used to capture and categorize information about the COVID-19 pandemic, students' experiences accessing the internet during the pandemic, internet access methods, internet use, and knowledge of cyber fraud. It also captures if students had any training on cyber fraud.	0	0
Covid-19	Is used to code any information relating to the COVID-19 pandemic and the online experiences of students during this period. We can gain a better understanding of how students accessed the internet and their experiences during this time, which can help us to understand how the COVID-19 pandemic affected students' online experiences and well-being.	29	67
Experience	This code is used to capture the experiences of students' ability to access the internet during the COVID-19 pandemic.	25	41
Internet Access and usage	This code captures and categorizes information related to the use of internet technologies, including what devices are used to access the internet, how these devices access the internet, what students use the internet for, and how often the internet is used.	0	0
Computer and Laptop	This code provides additional information regarding whether students possess any computing devices besides mobile phones.	24	25
Internet Access Medium	Provides more information on how these devices access the internet: This can include mobile data and fibre optic connections.	27	58
Internet Usage	Provides more information on what the internet is used for: This can include activities such as browsing the web, online shopping, research, and using social media.	30	86
Mobile Phone	Provides more information on whether the student is using their phone to access the internet.	29	42
Period	Provides more information on how often the internet is used: This can be measured in terms of daily, weekly, or monthly.	29	32

Name	Description	Files	References
Security Measures	Provides more information on the security measures that students use to protect themselves from various threats.	30	55
Knowledge of cyber fraud	This code examines the details of participants knowledge of Cyber Fraud	30	60
Training	This code examines if students received any training	24	32
Cyber fraud Incident	This code examines the details of the cyber fraud, including the realization of the fraud, the events or circumstances that led to it, time to resolve, additional financial losses, awareness of others affected, challenges, support received, resolution, and satisfaction.	7	14
Application for Funding	This code analyses if the student received help with their financial aid application.	28	68
Assistance received satisfaction	This code analyses the student's satisfaction with the resolution received from the financial aid office, police station, or college regarding the cyber fraud incident.	24	36
Contract	This code checks if the student received a contract that states the amount of funds they will receive.	10	13
Extra Mile	When somebody went further to try and resolve their own case	1	1
Extra money spent	This code checks whether the student incurred additional expenses (out of pocket) to resolve the cyber fraud incident.	17	21
Inconvenience	This code checks whether the student experienced any other inconveniences due to the cyber fraud incident.	4	4
Know of any others affected	Does the student have knowledge of anyone else who has been affected by cyber fraud?	14	18
Realization of Fraud	This code examines how the student became aware that they were victims of cyber fraud.	30	66
Events or Circumstances	This code captures the events or circumstances that led to the cyber fraud.	26	74

Name	Description	Files	References
Reporting	This code checks whether the student reported the cyber fraud to various institutions, including the financial aid office, police, or college.	9	14
College	This code checks whether the student reported the cyber fraud to the college.	28	46
Financial Aid Institution	This code checks whether the student reported the cyber fraud to the financial aid institution.	29	69
Police	This code checks whether the student reported the cyber fraud to the police.	29	60
Resolution	This code attempts to determine if the student was able to resolve the incident with the various institutions.	16	23
Support	This code attempts to determine if the student received any support from friends, family, or other sources after the cyber fraud.	23	45
Time Spent	This code aims to understand the amount of time the student spent attempting to resolve the cyber fraud incident.	29	56
Effect of Cyber Fraud	This code aims to understand the effect of the cyber fraud on the student.	5	5
Behavioural	This code examines the behavioural effect.	29	54
Education	This code examines the effect of cyber fraud on the students' education.	6	7
Completion	This code examines whether the student managed to complete their course.	21	32
Grades	This code examines whether the cyber fraud had any effect on the students' grades	15	21
Emotional	This code examines the emotional effect.	30	67
Financial	This code examines the financial effect.	19	28
Borrowed	This code checks if the student has borrowed any money due to cyber fraud.	2	3
Money Lost	This code checks if any money was lost due to cyber fraud, and if so, how much.	30	81
Physical	This code examines the physical effect.	20	26

Name	Description	Files	References
Psychological	This code examines the psychological effect.	28	56

8.6 Appendix F – Ethical Clearance

Faculty of Commerce

Private Bag X3, Rondebosch, 7701
2.26 Leslie Commerce Building, Upper Campus
Tel: +27 (0) 21 650 4375/ 5748 Fax: +27 (0) 21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Internet: www.uct.ac.za
@Commerce UCT **UCT Commerce Faculty Office**

23 11 2022

Gershon Hutchinson

Department of Information Systems

University of Cape Town

REF: REC 2022/11/011

The Impact of Cyber Fraud on Higher Education Financial Aid students in South Africa

We are pleased to inform you that your ethics application has been approved. Unless otherwise specified this ethical clearance is valid until 31-Dec-2023 .

Your clearance may be renewed upon application.

Please be aware that you need to notify the Ethics Committee immediately should any aspect of your study regarding the engagement with participants as approved in this application, change. This may include aspects such as changes to the research design, questionnaires, or choice of participants.

The ongoing ethical conduct throughout the duration of the study remains the responsibility of the principal investigator.

We wish you well for your research.

2022.11.23
17:36:04 +02'00'

Jacques Rousseau
Commerce Research Ethics Chair
University of Cape Town
Commerce Faculty Office
Room 2.26 | Leslie Commerce Building

Office Telephone: +27 (0)21 650 2695 / 4375
Office Fax: +27 (0)21 650 4369
E-mail: jacques.rousseau@uct.ac.za
Website: http://www.commerce.uct.ac.za/com/Ethics-in-Research

8.7 Appendix G – Interview Questions

		Interview Questions	References
Theme		**Question**	
Demographic Information	Gender and Age	• How old are you? • What is your gender? [M/F/Other/Prefer not to answer] (Note: psychosocial cybercrimes are more gendered than socio-economic cybercrime, suggesting problems with the meaning of 'cyber-enabled crimes (Lazarus et al., 2022).	Abdulai (2020) Lazarus et al. (2022) Agrafiotis et al., (2018)
	Education and knowledge of cyber fraud	• What is your highest qualification? • Have you been trained on issues of cyber fraud? And if so, in which program or course? Please elaborate. (Note: there is a positive and significant relationship between cyber fraud investigation and computer forensic education, digital forensic education, law enforcement education and seminars, workshop and conferences (Abu, Lateef, & Echobu 2018))	
Contextual Background	Internet Access and usage	• How do you access the internet? – (mobile phone/laptop/desktop/or) • What security measures do you employ on your devices to protect against cybercrime in general? • What factors affect or influence how you *access* the internet? • How often do you use the internet and related technologies? • What factors affect or influence how you *use* the internet?	Button and Cross (2017)
	COVID-19 Context	• How has the effect of COVID-19 (such as its social stigma) affected you psychologically, your behaviour and your emotions towards internet use or reliance on the internet to perform your activities? (Note: Cybercriminals target victims' psychological vulnerabilities, taking advantage of COVID-19-related anxiety by manipulating emotional instabilities to enable cyber fraud)	Ma and McKinnon (2022)
	Perception of cybercrime	• What is your understanding of the term *Cyber fraud*?	Button and Cross (2017) Button et al. (2021)
Effect of cyber fraud	Cybercrime incident	• What online transactions/activities do you engage in and why? • At what point during the transaction did you perceive cyber fraud and how did you detect it? • Explain how you dealt with the cyber fraud incident and what assistance you received, if any, from the online platform, individual or institution? • What effect (if any) has cyber fraud affected you and explain how it has affected you:	Button and Cross (2017) Button et al. (2021)
	Cybercrime effect	○ Financially. (Note: In general, fraud reporting appears to involve a rational component because financial and non-financial harms and the expected utility of reporting are more relevant to the decision than socio-demographic factors (Kemp, 2022) ○ Your (Consumer) Confidence ○ Changes in habits	Siahaan and Nasution (2018) Kemp (2022) Button and Cross (2017) Button et al. (2021)
		○ Emotional and Psychological ○ Social and societal	Agrafiotis et al., (2018) Cross (2019) Button and Cross (2017)

			Button et al. (2021)
		○ Behavioural ○ Physical	Button et al. (2021) Button and Cross (2017) Button et al. (2021a)