The effectiveness of the South African Smart ID card

Fighting digital identity fraud.

Tshepo Magoma

Yoti Fellowship Programme

Contents

Author

Tshepo Magoma

Tshepo is a South African-born researcher, strategist and innovator with a track record working in Africa's small business and social enterprise sectors. He is particularly interested in digitisation on the continent and is a subject-matter expert in disruptive innovation. He is an advocate for youth entrepreneurship and has worked widely in the NGO sector.

Tshepo is also a published academic and has been a speaker, facilitator and panellist at numerous events and meetings of the African Union, the Africa Research Group, the Innovation Hub, ISPA iWeek 2019, and the World Youth Forum in Egypt.

Published by Yoti

This is an Open Educational Resource (OER) and is an outcome of the Yoti Digital Identity Fellowship awarded to Tshepo Magoma during 2019 – 2020, supported by Yoti under its Social Purpose programme.

License

Attribution

Executive Summary

Background

Growing trends in identity fraud have propelled South Africa to change its ID system. The government opted for a Smart ID card that promised to be fraud-proof, unlike the previous green ID book which was relatively easy to manipulate. However, cases of identity fraud have increased despite the introduction of the Smart ID card. South Africa's digital ID fraud has grown exponentially during the COVID-19 pandemic, prompting the need for key decision-makers across both the public and private sectors to seek solutions to curb this alarming trend.

Objective

This study's purpose was to determine the effectiveness of the South African Smart ID card in fighting identity fraud. Since its introduction, many cases of fraud have been reported, including fraudulent marriages and identity theft. The South African government, however, has remained hopeful that the Smart ID card is incorruptible, and believes that the most recent fraud has been carried out using the previous green ID books. This study aims to uncover all aspects of the Smart ID card features that are essential in fighting identity fraud and will also make further recommendations about the Smart ID card system in support of continuing efforts to combat all kinds of fraud.

Method

Quantitative data were collected using an online questionnaire which was sent to 500 participants using the SurveyMonkey software. Of these participants, 200 were government officials, 100 were industry experts, 100 were fraud victims, and 100 were participants randomly selected from schools and their respective communities. For data analysis, this research made use of SPSS software and Microsoft Excel.

Results

The findings of this research confirmed that identity fraud is a growing problem in South Africa. The lack of proper guidance regarding the discontinuation of the old green ID book also contributes to the problem. The pandemic has also exposed the inefficiency of the South African government in its distribution of government services. To a large extent, fraudulent activity arose from the use of fabricated IDs and the lack of tools to verify IDs and to authenticate people.

Conclusion and recommendations

The research concludes that the Smart ID card, on its own, is not effective in the fight against identity fraud. Future solutions to this problem, that can enable verification and ease authentication, will be pivotal in fighting fraud in South Africa. The study also recommends that the government should increase the level of awareness around the consequences of ID theft, look into consulting with all groups, including rural communities, and introduce user-friendly systems that can be rolled out efficiently and effectively.

Keywords: Smart ID; Green ID; Identity Fraud; Digital ID; DHA; Blockchain.

1. Introduction

Digital identity traditionally refers to an amalgamation of all available attributes and information that can link an online persona to a physical person. Digital identity is increasingly the focus of policy discussions in many countries, including South Africa. Several governments are proposing or implementing national digital identity programmes, with multilateral institutions making investments in order to fund them (Lile, 2017).

In South Africa, the Department of Home Affairs (DHA) started replacing the previous green barcoded identity documents (IDs) with Smart ID cards on the 18th of July 2013. The Smart ID cards were considered to have better security features, such as an optically variable device, optically variable ink, Line ID and a PDF417-type barcode, which is deemed extremely difficult to forge. However, there are still many reported cases of fraudulent activities involving identity; these include identity theft, identity scams and faked marriages (Li, 2017).

In recent years, ID fraud has been widely reported in the South African media and is seen as a significant and rising threat. There has been agreement among government and private sector organisations, including the South African Fraud Prevention Service (SAFPS), Customer Profile Bureau (CPB), National Credit Bureau (NCB), and Alexander Forbes Insurance (AFI) that ID theft is a serious issue (Junie, 2019).

Despite several allegations, the Department of Home Affairs (DHA) maintains its initial stance that introducing the Smart ID card remains the best solution to the challenges that were experienced previously with the manipulation of the application processes for the green, barcoded ID book. The shift to a Smart ID card system was intended to eliminate fraud but recent experience has shown that there are shortcomings (Kamble, 2018).

This research determines the effectiveness of the South African Smart ID card in fighting digital identity fraud and also paves a way for future national digital identity programmes that should have a human rights perspective. The United Nations' Sustainable Development Goal 16.9 states that, by 2030, countries should 'provide legal identity for all, including free birth registrations'. This process can be enhanced by building policies in legal and technological frameworks (BusinessTech, 2019b) that are directed towards achieving SDG Goal 16.9. Such policies can create an ecosystem in which digital identity systems can be promoted in South Africa.

The current study discusses the context of the debate about these initiatives, globally, and proposes safeguards and policy recommendations for those involved, including public officials, lawmakers, representatives from judicial and human rights institutions, technologists, officers of development institutions, and members of the private sector.

2. Background

The evolution and landscape of identity in South Africa are complex. The following literature review should help provide an understanding of the nature and meaning of the problem (Saunders and Lewis, 2012).

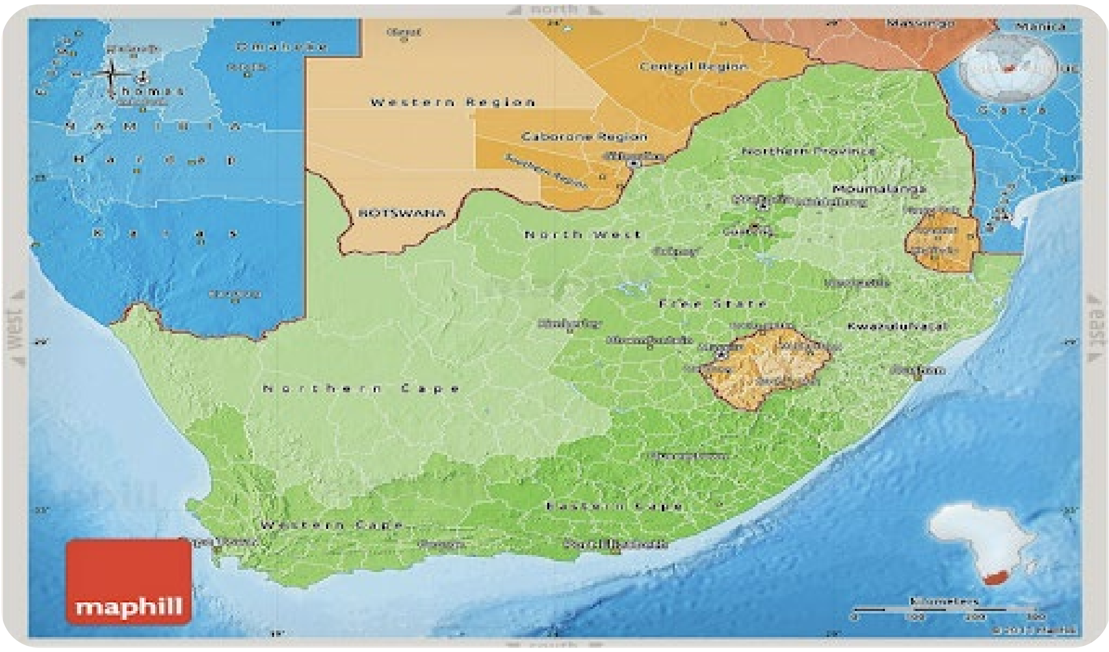


Figure 1: Map of South Africa

The Republic of South Africa (RSA) has a population of over 51 million people, living in nine provinces, which differ in size (Figure 1). The smallest province is the tiny and crowded Gauteng, a highly urbanised region that includes the cities of Johannesburg and Pretoria. The largest province is the vast, arid and empty Northern Cape, which occupies almost a third of South Africa's total land area. The country has common boundaries with Namibia, Botswana, Zimbabwe and Mozambique and citizens of these countries often enter South Africa to seek work. In order to obtain employment in South Africa, one has to present a South African ID document and foreign nationals often resort to acquiring false IDs in order to get a job. South Africa is a vast economic hub that houses many foreigners and immigrants from other African countries (SABRIC, 2018).

There are several drivers of identity fraud in South Africa. For citizens of other countries in Africa, obtaining South African permanent residence is seen as a pathway to a better life. In addition, people may use IDs belonging to other people in order to claim government social grants. Given the levels of poverty in the country, ID theft is increasingly used to defraud people or to obtain state benefits (Kaplan, 2017). Identity theft is also used by criminals to escape criminal prosecution and to help them flee to neighbouring countries. People also resort to forging death documentation in order to collect life insurance policies or engage in ghosting (taking on the identity of a deceased person). Several studies have also indicated that law enforcement has been slow to address this new criminal trend – often victims of ID fraud are unaware of the crime perpetrated against them and it is only after they become aware that the perpetrator may be sought or apprehended (Khambule, 2018).

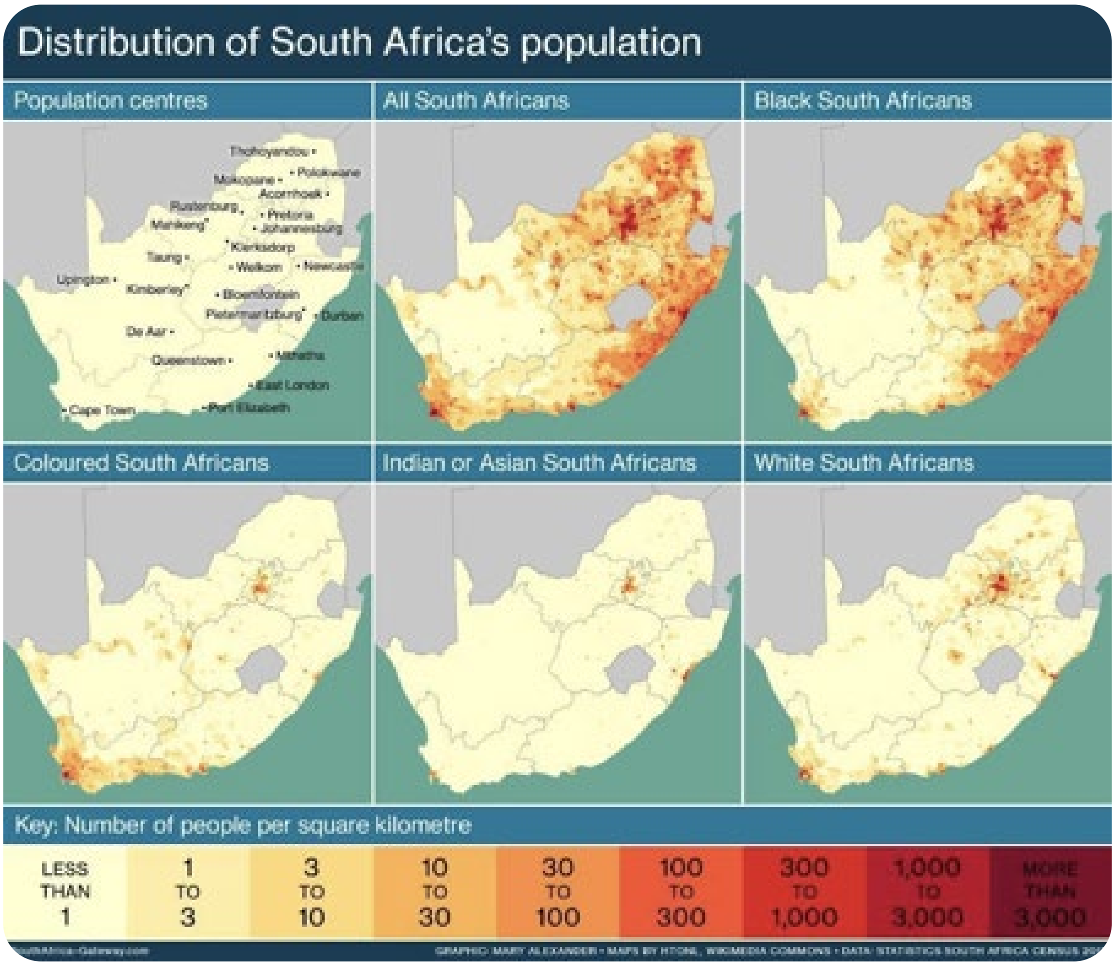


Figure 2: Distribution of South African population (2011)

According to the census of 2011 (Statistics South Africa, 2012), black South Africans make up the majority (79%) of the population and live both in the cities and across the poorer rural areas. Indian and Asian South Africans form the smallest minority (2.5%) of the population. They are concentrated in the cities of Durban, Johannesburg and Cape Town. Coloured people (mixed race) live mostly in the Western and Eastern Cape, both in the cities and in the rural areas. Whites make up 8.9% of the population and live mostly in the cities. The rise of urbanisation fuelled by lack of infrastructure, facilities, and opportunities in South Africa has led to the majority of people originally from the countryside to concentrate in Gauteng Province. The Province has become the economic heart of the country, with over a quarter of the nation living across its metropolitan areas. It is not surprising, therefore, that most digital fraud occurs in the metropolitan urbanised areas, particularly in Gauteng and the Western Cape (Khambule, 2018).

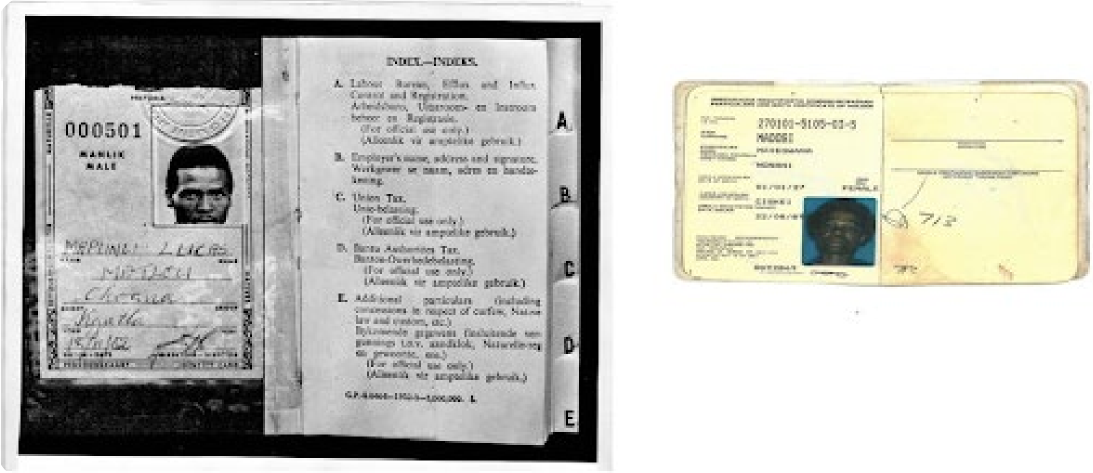
2.1 Evolution of ID Documentation in South Africa

The South African ID system has evolved over the years. Changes were initially made as a result of the shift from the apartheid regime to a democratic nation that sought to uphold the dignity of its people by providing them with comprehensive ID documents. Subsequent changes were made because of the need for a more secure ID that could reverse the trend of increasing ID theft and fraud. Azhar (2017) states that ID theft has become such a widespread threat to human security that the subject pervades current popular culture. ID theft costs South Africa more than R1 billion every year, according to a major credit bureau and a national insurance organisation.

2.1.1 Apartheid-era Identity

In South Africa, the Pass Laws of 1952 compelled black South Africans to carry a pass book (ID); this internal passport system was designed to segregate and control the population (Kamble, 2018). Like a passport, the pass book (Figure 3) contained the individual's fingerprints, photograph, employment details, racial classification, and the area in which he or she was allowed to live and work (Kamble, 2018). Pass Laws severely limited the movements of black South African citizens by requiring them to carry a pass book, also known as a ‘dompas’ (literally, dumb pass), when outside their homelands or designated areas (Lele, 2017).

Forgetting to carry a dompas resulted in arrest and expulsion out of 'white' South Africa into a 'homeland', or reserve. Each year, over 125,000 blacks were arrested for technicalities regarding a dompas. In 1956, twenty thousand women marched to the Union Buildings in Pretoria to protest against the detested passbooks (Lele, 2017). The pass book became one of the most hated symbols of the country's apartheid system until the requirement was effectively lifted in 1986.



INDEX—INDEKS.

A. Labour Bureau, Influx and Influx Control and Registration.
Arbeidsburo, Uitsorteer- en Instroombeheer en Registrasie.
(For official use only.)
(Alleenlik vir amptelike gebruik.)

B. Employer's name, address and signature.
Werkgewer se naam, adres en handtekening.

C. Union Tax.
Unie-belasting.
(For official use only.)
(Alleenlik vir amptelike gebruik.)

D. Bantu Authorities Tax.
Bantoe-Owerheidsbelasting.
(For official use only.)
(Alleenlik vir amptelike gebruik.)

E. Additional particulars (including concessions in respect of curfew, Native law and custom, etc.)
Bykomende gegewens (insluitende vergunnings t.o.v. aandklok, Naturellereg en gewoonte, ens.)
(For official use only.)
(Alleenlik vir amptelike gebruik.)

Figure 3: Pass book (Apartheid-era identity) 1960–1986

2.1.2 The Green ID Book

When South Africans lined up in their millions to vote during their first democratic elections in 1994, they all carried with them an ID to verify who they were. The green identity book (Figure 4) was introduced, post-1994, as a compulsory ID document for all South African citizens above 16 years of age.

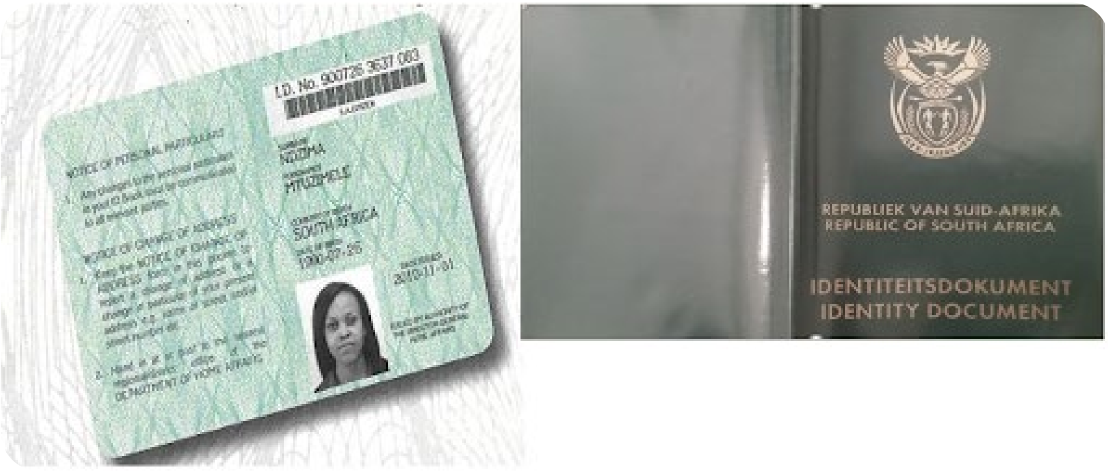


Figure 4: The green ID book

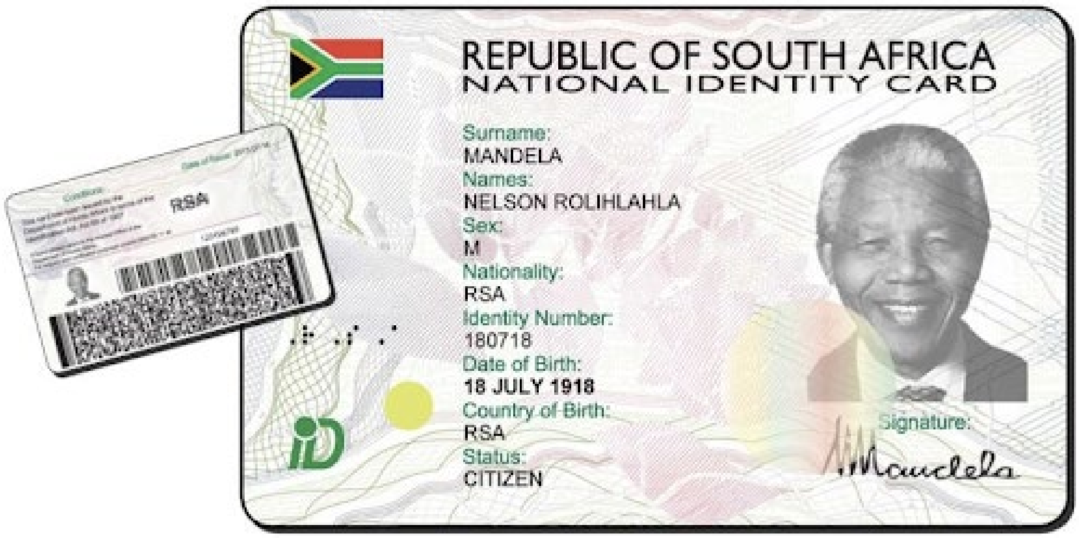
This ID document was designed like a book, with a line barcode and a unique 13-digit ID number at the top. It featured a photographic image that could be taken separately by any photographer; this image was then inserted into the book by Home Affairs officials and was sealed and covered with plastic. This system proved to be vulnerable to fraud and theft. Fraudsters could easily remove the owner's image from the top cover and insert their own, thereafter conducting unauthorised transactions on behalf of the owner. The 13-digit identification number was also used to secure a driver's licence as well as licenses for firearms (Ruppar, 2005), so the theft of such a document could have far-reaching consequences.

In 2000 the Department of Home Affairs introduced specific changes to the green ID book to make it more secure. The new coat of arms appeared on the ID, and the photograph, which had been pasted in, was now digitally printed in black and white on the first page (Lele, 2017). The second-generation green ID was subsequently replaced by a new Smart ID card containing a microchip embedded with biometric security features from July 2013.

2.1.3 Smart ID Card

After many years of using a green ID book with limited security features, South Africa finally upgraded to what it is called a 'Smart ID card', which is on a par with identity systems used in Europe, Asia and America. The new card was launched on the 18th of July 2013, the 95th birthday of Nelson

Mandela, who was one of the first to receive his Smart ID card (Figure 5). The small, credit card-sized piece of polycarbonate carries much information. It is a precursor to paperless government and a restorer of dignity and common citizenship (Hanvey, 2018).



REPUBLIC OF SOUTH AFRICA
NATIONAL IDENTITY CARD

Surname:
MANDELA
Names:
NELSON ROLIHLAHLA
Sex:
M
Nationality:
RSA
Identity Number:
180718
Date of Birth:
18 JULY 1918
Country of Birth:
RSA
Status:
CITIZEN

Signature:
NMandela

Figure 5: The Smart ID card

The South African Smart ID card effectively replaced the old green barcoded identity book. Both are identity documents that include the holder's photograph, full name, date of birth, place of birth and identity number. South African ID documents also record evidence of the holder's voting in local and national elections (Lele, 2017). Despite being introduced in 2013, South African citizens born outside of South Africa cannot apply for the Smart ID card, nor can they access the online services of Home Affairs (as of November 2020). For identity purposes, such applicants still only receive the old green ID book.

The Smart ID card is intended to be used as a multipurpose ID to which government departments can upload their data via the microchip present on the card. The Smart ID card represents a sophisticated system of data management as well as being a precursor for eliminating paperwork in government operations (Thompson, 2020). It is a quantum leap from its predecessor in terms of secure technology and goes a long way towards preventing identity theft and fraud. The current information on the Smart ID card chip is laser-engraved to prevent tampering and this was proposed as a way to cut down on the fraudulent use of fake or stolen IDs that characterised the era of the green ID book.

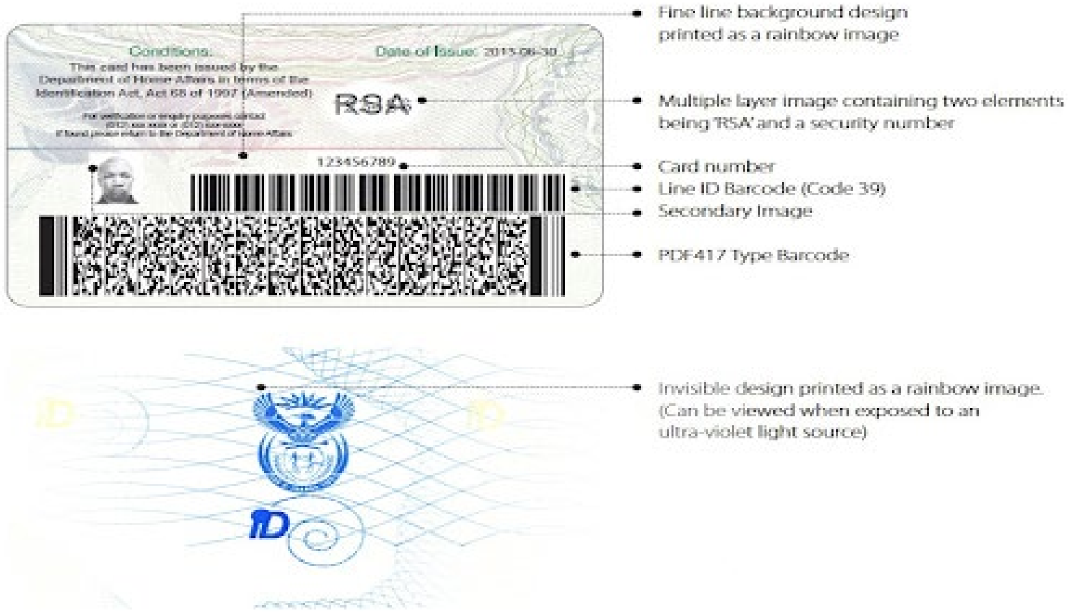

Conditions:
This card has been issued by the Department of Home Affairs in terms of the Identification Act, Act 68 of 1997 (Amended)
Date of Issue: 2013-06-30
RSA
123456789
ID
ID
ID
Fine line background design printed as a rainbow image
Multiple layer image containing two elements being 'RSA' and a security number
Card number
Line ID Barcode (Code 39)
Secondary Image
PDF417 Type Barcode
Invisible design printed as a rainbow image. (Can be viewed when exposed to an ultra-violet light source)

Figure 6: Smart ID card (reverse side)

The owner's photograph is laser-engraved and has a background of lines printed like a rainbow, which makes it difficult for fraudsters to forge (Jenna, 2020). The card has optical security in the form of an optical variable device (OVD); it has a colour-shifting motif and a coat of arms that are not overtly visible but that fluoresce when exposed to UV light. The card has text written in braille that is easy to feel. The card's reverse side also has a photo and 'RSA' text that is printed above a security number. A microchip 80kb in size is used to provide security as it carries the fingerprint, photo, and owner's name. The reverse side also shows a line code for the owner's ID number and a 2D PDF417-type barcode. The Department of Home Affairs has said that it is likely to be able to produce three million ID cards a year.

2.1.4 The Smart ID Card System

Proponents of Smart ID card programmes argue that they bring benefits such as more accurate and efficient delivery of government services. Critics have noted that national Smart ID card schemes may not ensure more effective distribution of benefits, better service delivery, or improved governance (Junie, 2019). The development of digital identities will have to assuage growing concerns that government entities could use a digital

ID to conduct mass surveillance of the population. Since its inception, many cases of fraudulent marriages and identity theft have been reported. However, the South African government has remained resolute that this Smart ID card is incorruptible and claims that cases of identity fraud could only involve the previous green barcoded ID book.

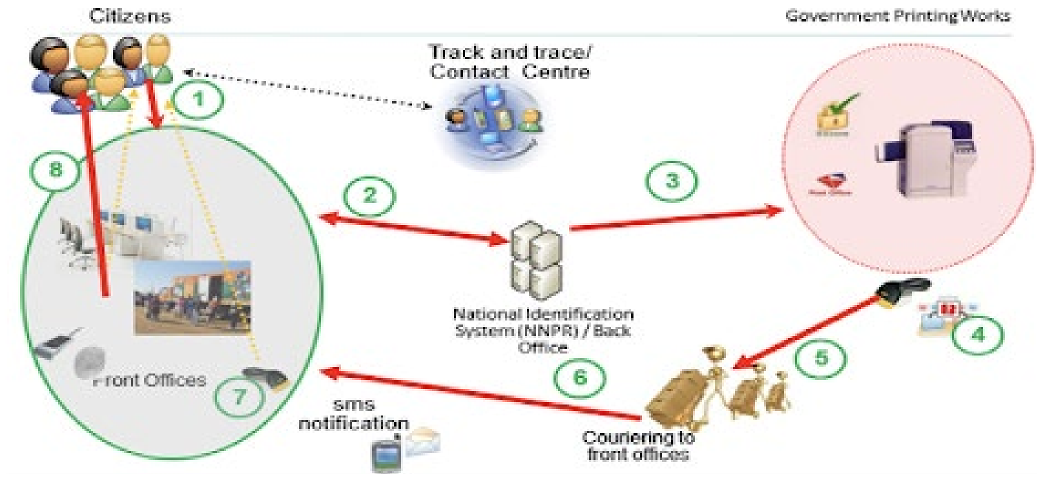

Citizens
Government Printing Works
Track and trace/
Contact Centre
1
2
3
4
5
6
7
8
National Identification System (NNPR) / Back Office
Front Offices
sms notification
Couriering to front offices

Figure 7: Smart ID card life cycle (Source: DHA)

The delivery time for the old green ID book was about 54 days following application. The new smartcard process takes only three days. Following research into national eID programmes implemented by governments across the world, the Department of Home Affairs opted for an ID system that has a high level of security and advanced data-protection mechanisms.

In South Africa, two means of authentication are used – biometric fingerprint verification or a pin code that is known only to the user. Embedded secure software with its microprocessor protects identification details. This ensures that only authorised authorities can read and verify the card's data using contactless machine-readable scanners. The inclusion of this biometric identification supposedly makes it virtually impossible to duplicate the card. It ensures, for the first time, that citizens can be securely authenticated (Lele, 2017).

2.2 The Landscape of ID Fraud

Identity fraud is broadly defined, according to Junie (2019), as an offence covering any fraudulent use of personal data. ID fraudsters not only take a person's money but may also damage the person's good reputation. South Africa is ranked the world's third highest in terms of economic crimes recorded, with corruption and bribery accounting for 42% of consumer crimes since 2019 (PwC's Global Economic Crime and Fraud Survey, 2020).

Identity fraud is therefore frighteningly common in South Africa. Identity theft is more prominent in the provinces of Gauteng and KwaZulu-Natal (KZN) and, in total, costs South African companies more than R1 billion a year.

Several studies confirm the increased incidence of ID fraud in different countries, and especially in developing countries like South Africa. The misuse of identity data leads to abuse, robbing and other unauthorised access to finances. Junie (2019) finds that organisations to which the victims of identity fraud are linked are also victims in as much as they are affected financially by the fraud.

In support of this view, Rakololo and Maluleke (2020) say that the theft of IDs is a dual crime; it typically has two victims, both the person whose ID has been stolen and the organisation from which money has been stolen. Individuals are not always regarded as victims, since they may not be ultimately responsible for the financial loss that results. The need for key decision-makers in both government and private sectors to protect themselves from identity fraud is critical for a country already facing economic hardships and marred by accusations of corrupt COVID-19 contracts with government officials.

Shockingly, during the COVID-19 pandemic in 2020, identity fraud cost South Africa over R1 billion (Cape Business News, 2020). This was largely due to money claimed from the TERS (Temporary Employee/Employer Relief Scheme) through fraudulent applications that could have been prevented with the correct ID authentication. The aforementioned article states that R30 million of the TERS fund was paid to persons with invalid identification numbers, R696 million to refugees who had not made UIF contributions in the past year, and an astonishing amount of R440 000 was paid out to people who were dead.

ID fraud usually occurs without the victim knowing and often it's a year or more before victims realise. Sometimes, people have even been imprisoned for crimes committed using their identities. Many victims report that the person who stole their identity is someone they know – such as a neighbour, roommate, or co-worker. Aside from financial losses, ID theft can also be emotionally draining and time-consuming. According to Rakololo and Maluleke (2020) corporations find it incredibly difficult to identify the individuals who commit such crimes, and often label them 'ghosts' since an unseen person hides behind a real person's identity.

2.3 The Future of Digital Identity in South Africa

Focusing on one centralised, directly administered national identity system prevents the formation and competitive use of multiple forms of identity and could lead to more efficient and empowering outcomes for users. Some argue that government policy should focus on encouraging the development of a variety of identification and credentialing systems, instead of insisting on its own issued national identity. In such a system, governments should accept any card or device that provides sufficient proof of the information required for a transaction (Lele, 2017).

For a developing nation like South Africa, government-administered or coordinated programmes aim to provide a single digital identity. Many such programmes entail a push to collect, store, and use biometrics of individuals as the primary means of establishing and authenticating their identity. Proponents of centralised national ID programmes argue that they bring benefits such as more accurate and efficient delivery of government services, anti-poverty regimes and welfare schemes. Critics have noted that national digital identity schemes may not in fact ensure more effective distribution of benefits, better service delivery or improved governance (Kamble, 2018).

It is important to remember that, given the development of technology, it is far from settled that the best solution for verifying an individual's identity is a national digital identity system that requires centralised, biometric-based authentication. For example, some scholars propose the use of blockchain technologies to authenticate a user's identity. Since the data stored on the public chain is as-good-as impossible to change, a user need not provide biometric or other types of personal information to authenticate identity (McLoughlin, 2015).

In conclusion, for digital identity to be empowering in specific contexts, the technological, legal and policy frameworks must be built on a foundation of user agency and choice, informed consent, recognition of multiple forms of identity, space for anonymity, and respect for privacy.

3. Current Research Methodology

3.1 Introduction

The research aimed to establish the effectiveness of the South African Smart ID card in fighting digital identity fraud. This section provides details of the approach taken and the methods used in order to establish this effectiveness while, at the same time making the research reliable and valid. It was important that the participants represented the population being studied and that these participants were "not systematically different in any meaningful way from the overall group" (Saunders and Lewis, 2012). Additionally, this section details the ethical background of the data collection, which is essential to make the study results reliable (Saunders and Lewis, 2012). Under this heading, the philosophical worldview, research worldview, methodological decisions, research approach, research methodology and timelines are also considered.

3.2 Philosophical Paradigm

Positivism formed the philosophical viewpoint for the study as a scientific approach was used to test theories or beliefs regarding the success or failure of the Smart ID card. Since the focus was on assessing whether fraudulent activities had declined since introducing the Smart ID card in South Africa, positivism was seen as the most suitable research philosophy; it allowed conclusions to be drawn based on the scientific findings. This philosophy has been associated with a logical manner of extracting knowledge and has been essential for incorporating logical reasoning into the consideration of whether the Smart ID card has been successful in eliminating fraudulent activities.

3.3 Research Approach

This research used a pre-existing theory of digital identity and the diffusion of technology to investigate the effectiveness of Smart ID cards in fighting digital fraud. The study took a deductive approach to the research. This system provided logical ways of generalising the data to achieve the main aim and objectives of the study.

3.4 Research Strategy

A survey was chosen for gathering data regarding the topic because it is an extensively used method in research and can provide accurate data related to the research topic (Saunders, et al., 2009).

3.5 Time Horizon

The research was cross-sectional given the project had a specific date set for submission. Since the study had a time constraint, it was designed in a way that best suited the researcher's time allocation. The study's time allocation was also impacted by the developments and restrictions imposed during the COVID-19 pandemic.

3.6 Data Collection and Analysis

500 participants took part in the research survey. Among these, 200 participants were officials in public departments in several government entities and 100 were key players in the financial industry in southern Africa where the majority of the fraud usually takes place. The research also looked at fraud prevention-focused NGOs and private sector firms. A further 100 were victims of identity fraud and the remaining 100 participants were randomly selected from schools and their respective communities.

Sampling refers to the process that is used for selecting a portion of a population to take part in research (Saunders & Lewis, 2012). A non-probability sampling procedure was used to select the participants. This technique is based on the researcher's subjective judgement and is not random. In this case, convenient sampling (as a type of non-probability sampling) was employed; this involves selecting participants because they were easy to identify and access.

It was important to choose the right sample from the right population. Sampling refers to the process that is used for selecting a part of the population for carrying out its research (Saunders and Lewis, 2012).

Creswell and Creswell (2017) have defined non-probability sampling as a technique in which the samples are gathered by a process that does not require all the individuals to be selected. The sampling technique was convenient sampling vs. the non-probability sampling method in which a well-known public directory of names was used and only those individuals listed in public or private institutions were selected. The business directory was narrowed down to databases of fraud victims from the South African Police Services and the Department of Home Affairs were used to identify the 100 fraud victims.

Following pandemic protocols, the questionnaire was conducted strictly online and distributed to all participants considering all possible ethical issues of the research. A quantitative research method has been used in which primary method of data collection has been adopted. With respect to this, the data collection instrument chosen for the research is in the form of a questionnaire online survey which was sent to the respondents through SurveyMonkey. This approach allowed the researcher to see the research study from the perspective of the participants (Creswell, 2017). Data analysis involved the use of graphs and tables generated by Microsoft Excel spreadsheets and the Statistical Package for Social Science (SPSS). The findings are compared to results from previously conducted studies (Creswell, 2017).

3.7 Ethical Considerations

Ethics in research ensures that the investigation serves the interests of all people involved in the study (Creswell (2017). At the start of this study, a letter detailing the exact nature and aim of the research was sent to all participants. In addition, each participant signed a consent form before taking part. The questionnaire did not include any sensitive or personal questions and thus avoided violating participants' right to privacy. The primary method of data collection has been the quantitative analysis method. To this end, the selected data collection instrument in the form of an online survey questionnaire is sent to interviewees via SurveyMonkey. All the sources used for the research have been acknowledged.

3.8 Research Limitations

The main limitation of this study has been the time constraint that has prevented in-depth research into the broader subject area. In addition, the coronavirus pandemic made it impossible to visit the respondents personally and meant that certain provinces were not covered in depth due to lockdown regulations. Access to certain individuals and resources was considered pivotal in achieving the goal of this research. The results of this research are thus primarily based on the information that the researcher was able to collect and analyse, despite the limitations posed by hard lockdowns and social distancing introduced as measures to ease the pandemic situation.

4. Results and Analysis

This study was carried out with the help of quantitative research and primary data collection, as explained in the previous chapter. The sample size chosen for analysis was 500 respondents, and the response rate was 100%.

4.1 Research Demographic

Several key demographic characteristics were recorded during the study. They include the age, gender, years of service, and rank of participants. Figure 8 illustrates the distribution of participants selected for the study. The representation of government officials was double that of any other category of participant.

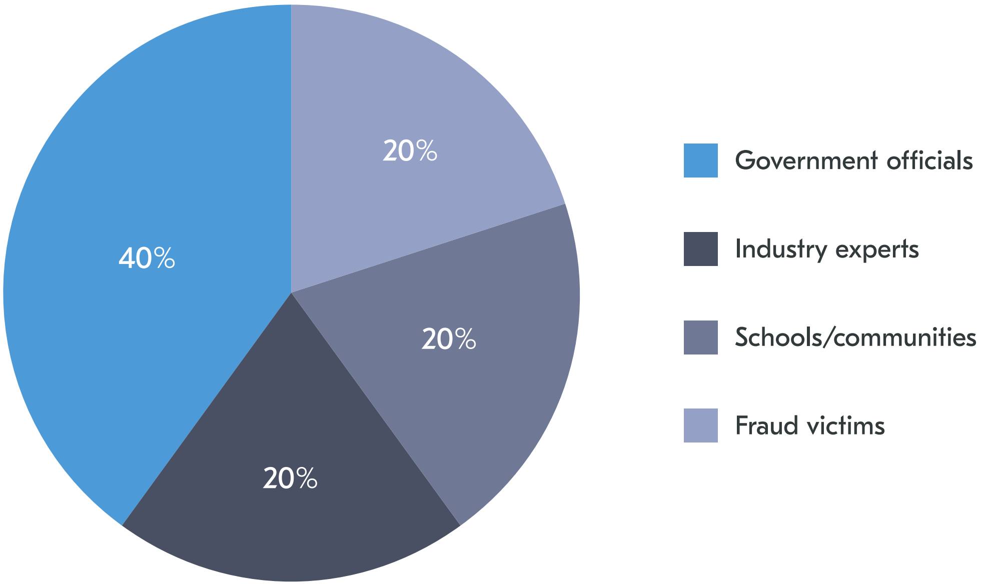


Figure 8: Participant classifications

In terms of years of experience for both government officials and industry experts, 85% of participants had more than five years of experience, and 65% had more than ten years of experience in their field (Figure 9).

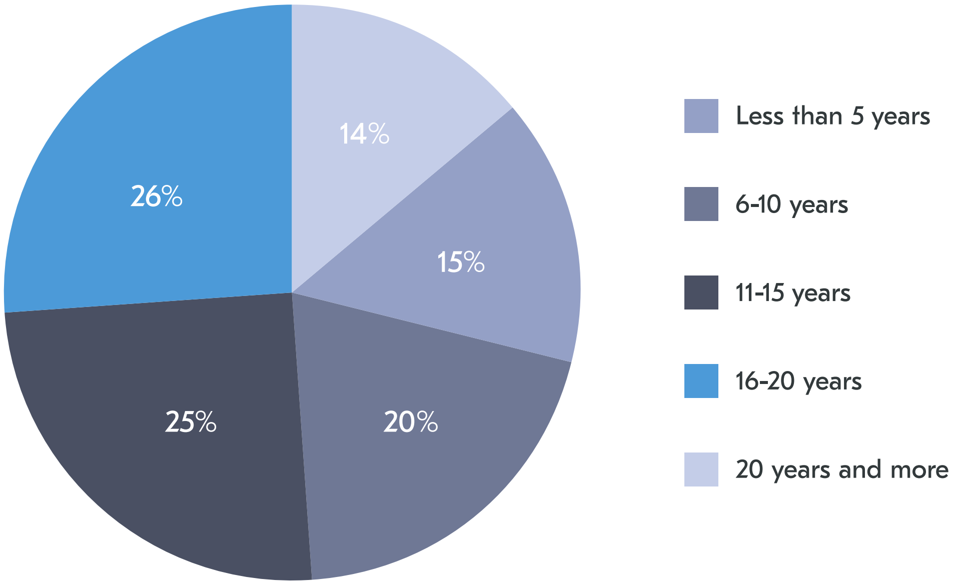


Figure 9: Levels of experience of participants who were government officials or industry experts

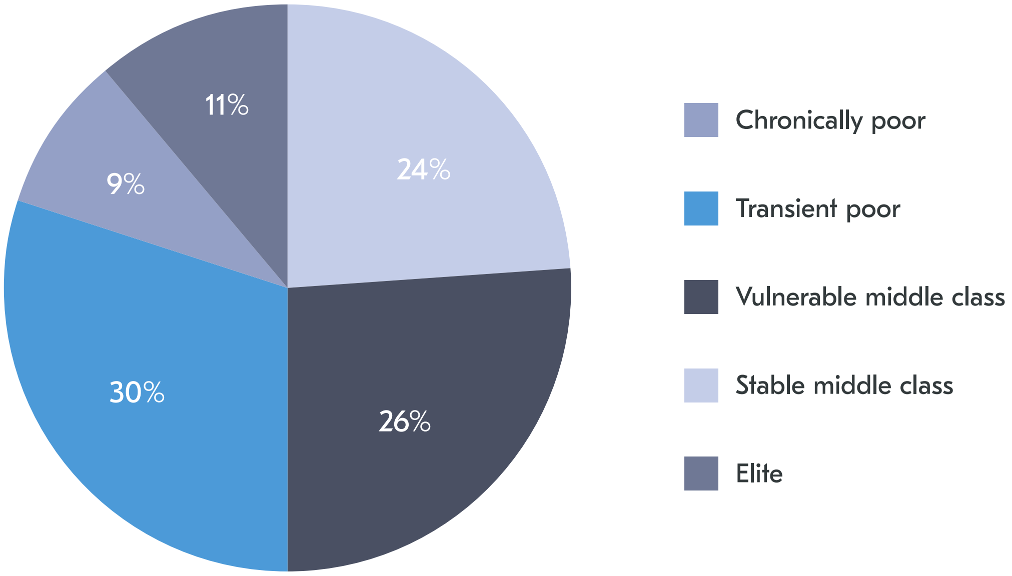


Figure 10: Socio-economic class of the research participants

Figure 10 presents details of the socio-economic standing of participants in this study. Approximately 50% of participants considered themselves to be middle class. Table 1 below shows the distribution of gender and age category of the research participants involved in the study. More females than males participated, and there was no participant who was younger than 18 or older than 65 years.

Research respondents' demographics				
	Age groups			
Gender	18–35 years	36–65 years	66+ years	**Total**
Male	20%	21%	(0%)	**41%**
Female	38%	21%	(0)%	**59%**
Total	**58%**	**42%**	**(0)%**	**100%**

Table 1: Gender and age category of participants

4.2 Questionnaire Results and Analysis

This section presents the frequency analysis of data obtained from the responses given to each question in the questionnaire (Willems, 2009; SPSS, 2020). Frequency analysis is regarded as an acceptable standard of data analysis for studies of limited scope. Due to the lack of awareness around various parts of this topic, participants were provided with background information that assisted them to answer the questions effectively. A total of 20 questions were asked in the questionnaire, and four variables were used in determining the key research question's themes, namely:

- The use of the green ID book and its advantages and disadvantages;
- Smart ID card and its effectiveness in fighting digital fraud;

- The landscape of digital fraud and the level of awareness therein;
- The developments around digital ID;

Figure 11 is derived from analysis of the answers given by the participants. The graph shows the responses to questions asking whether the participant knows someone, or knows of someone, who has been affected by identity theft.

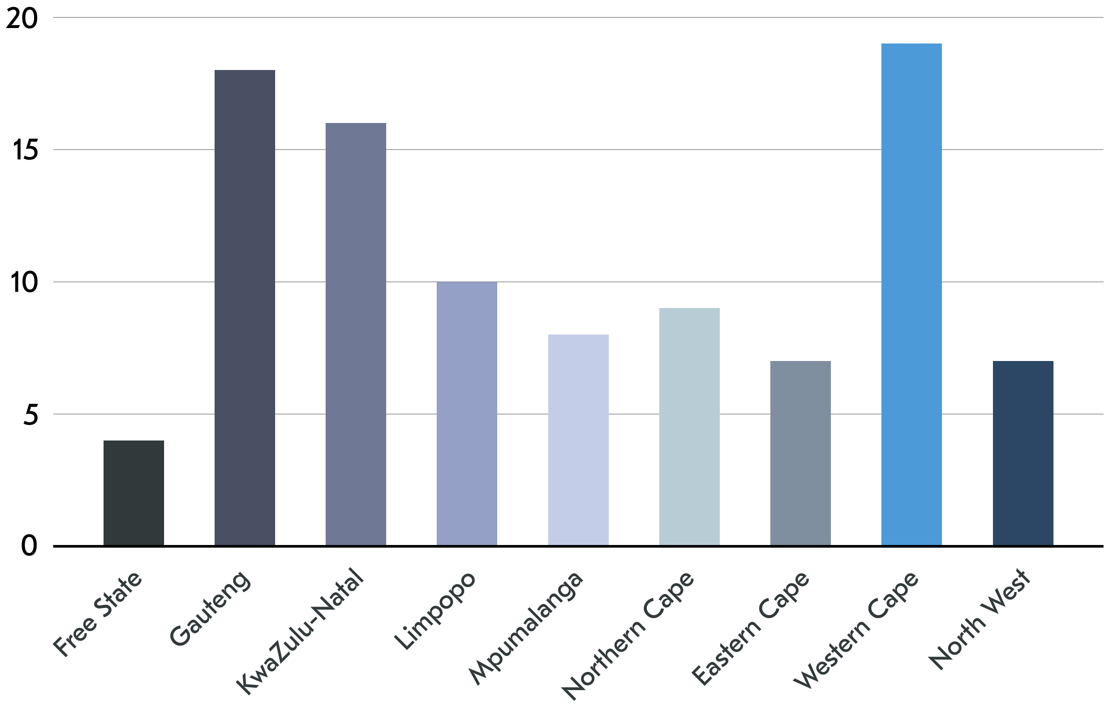


Figure 11: Number of participants knowing, or knowing of, an identity fraud victim

Figure 11 illustrates the frequency of identity theft across the South African provinces. Participants from Gauteng recorded most positive responses, with 90% stating that they knew, or had heard of, someone who was affected by identity theft. The Eastern Cape participants recorded the second-highest level of positive responses (80%), followed by the Free State and KwaZulu-Natal (both with 70%). The participants from Mpumalanga recorded 65% positive responses, while Limpopo participants recorded 60%. Participants from the Northern Cape and Northwest provinces recorded 55% and 45% respectively. This indicates that the problem of ID theft is more predominant in Gauteng province; this is as expected because of the province being the economic hub of the country.

The respondents also reported an increased spread of spoofed emails during the Coronavirus pandemic, emanating mostly from company websites offering relief payment aid because of economic challenges. More than 20% of the participants indicated that they continue to be contacted over the phone or even in person by such companies. 45% of the participants indicated the need for extensive awareness of digital fraud, since most of the economic activities in South Africa take place online. 36% of participants stated that, apart from fraudsters stealing victims' savings and running up massive debts, identity theft has proven to have long-term devastating impacts on credit reports and scores, and on business and personal relationships. It can wreak havoc on personal lives and financial wellbeing.

Apart from these impacts, the inconvenience and administrative efforts of dealing with identity theft can be significant, taking many months to resolve. Over this period, the victim can incur several incidental expenses, such as time off work, legal fees, and travel expenses. 32% of participants indicated that identity theft is more prevalent in South African townships and urbanised areas than in rural areas. In more rural communities, it is rare to find syndicates who sell replicated, fake IDs, as most of these syndicates operate in densely populated metropolitan areas. Identity theft takes different forms mostly in the rural and township communities. 44% of participants indicated that they had seen or heard of cases where people in these communities use fake IDs to obtain social grants and benefits from the state. The participants indicated that this issue is propelled by the lack of verification and authentication systems in state departments, and also by the socio-economic issues in these areas.

Overall, 67% of the participants had either been a victim of ID theft or knew someone who had. Of these, 28% said their identity theft occurred because of physical theft, 11% stated it was orchestrated by someone who was close to them and knew their personal details, 18% identified an online breach and 10% did not understand how their identity was stolen.

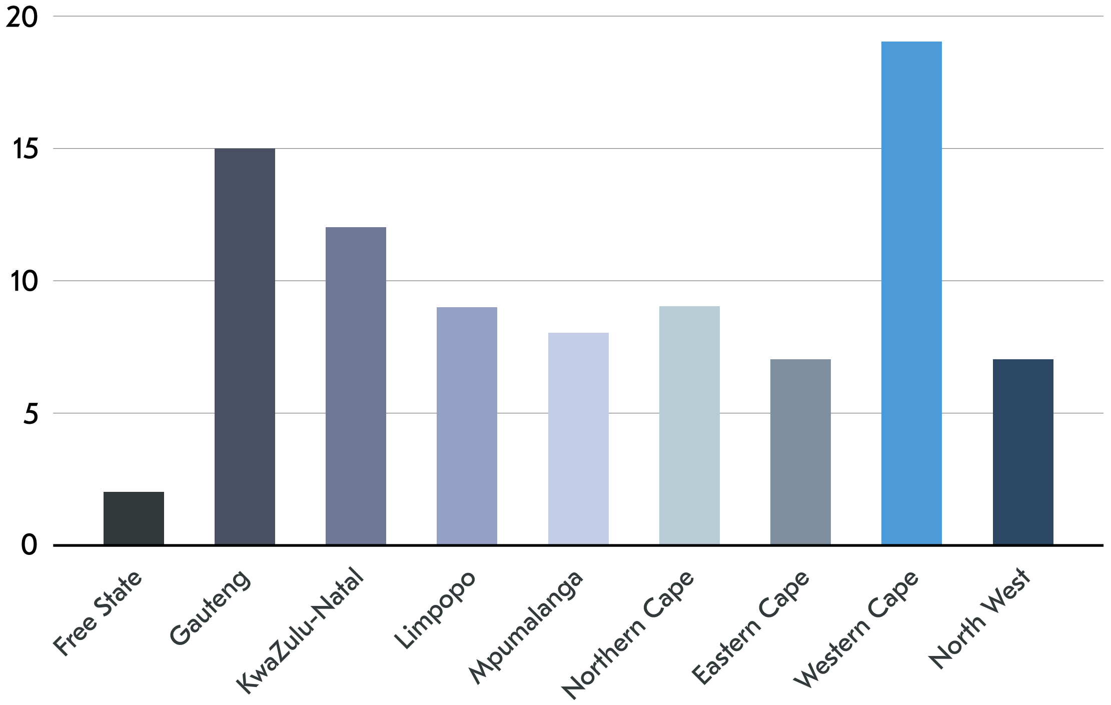


Figure 12: The level of awareness about ID fraud

When participants were asked whether they knew what a perpetrator of ID theft would do with the stolen ID card, there was a significant and worrying lack of awareness. Many people go about their daily lives, unaware that they are victims of fraud until they see the negative knock-on effect on their credit score. Some victims only find out about the theft of their identity when checking their credit report at the time of applying for a home loan or car finance. The researcher tested awareness of ID fraud among school learners, teachers, the elderly, the youth, and the government public officials. The results (Figure 12) indicate that people in the Northern Cape and the Eastern Cape are not fully aware of the potential consequences of ID theft; only 30% and 45% of participants, respectively, stated that they were aware. This is followed by the North West, Limpopo, and Mpumalanga provinces, which are also largely rural. In contrast, participants from Gauteng, KwaZulu-Natal and the Western Cape indicated high levels of awareness of the consequences of ID fraud. All these provinces have large cities and urban areas.

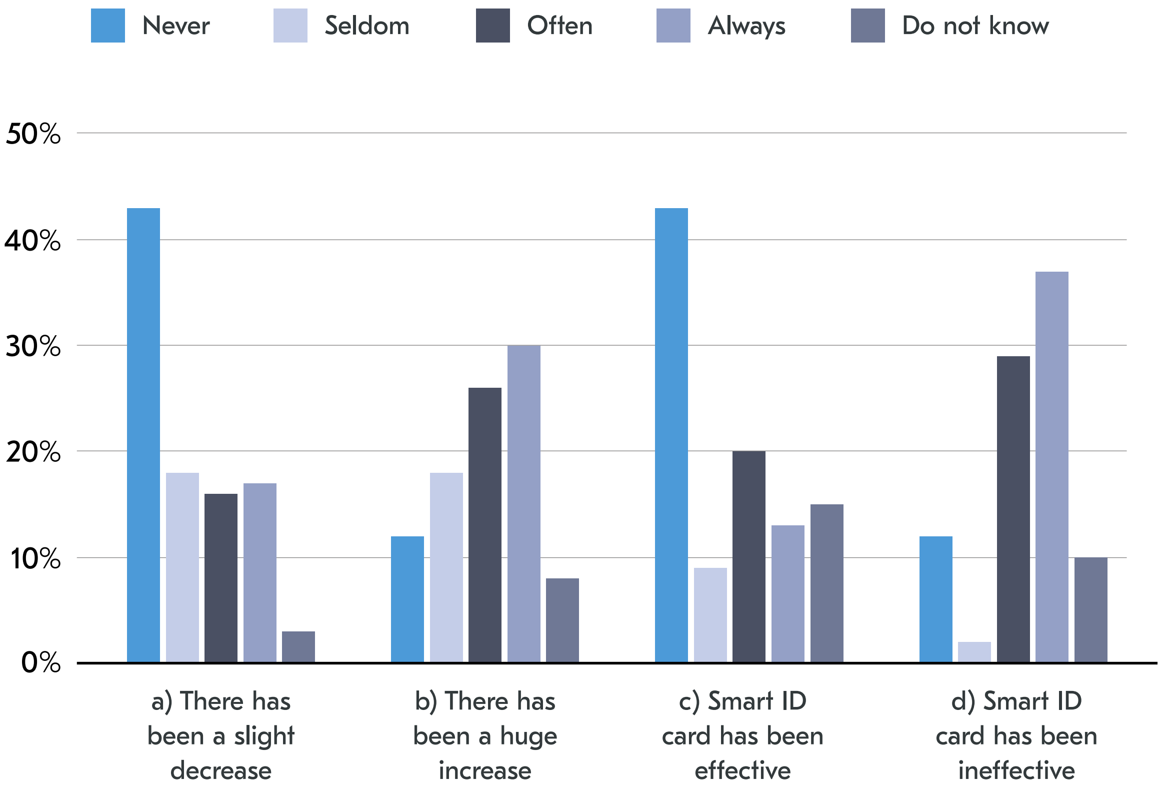


Figure 13: The effectiveness of the Smart ID card in fighting fraud

Participants were asked whether fraudulent activities had declined since the introduction of the Smart ID card in South Africa (Figure 13). The five options given to respondents were: Never, Seldom, Often, Always and Do not know. In column (a) above, they were asked whether fraud-related trends had changed since the introduction of the Smart ID card. In column (b) respondents were asked whether there has been an increase of fraud-related cases despite the introduction of the Smart ID card, and in column (c) they were asked whether they viewed the smart card as highly effective when fighting digital fraud. In column (d) they were asked whether participants viewed the Smart ID card to have always been ineffective (the question was asked to understand their concerns with the Smart ID card, and check if enhancements might be required).

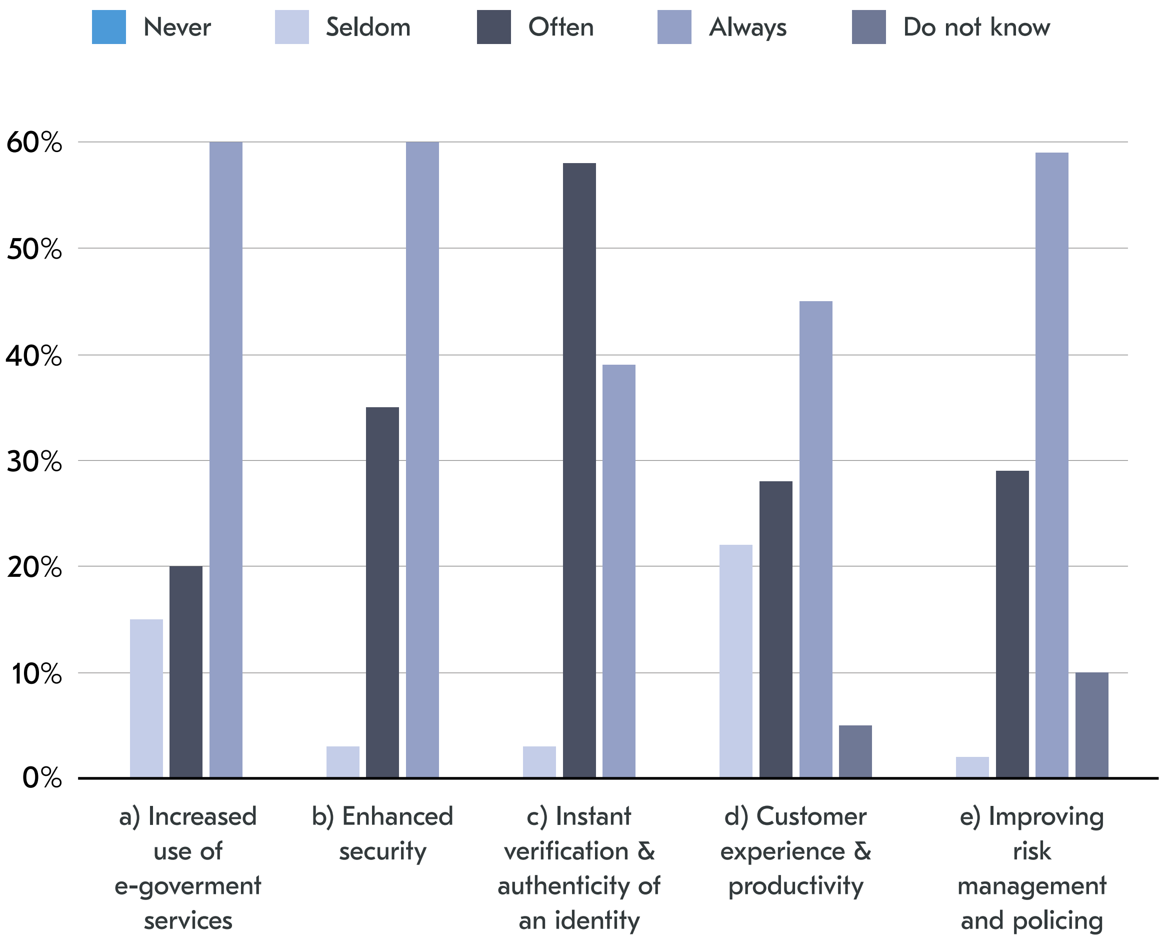


Figure 14: The future prospects of digital ID

Participants were also asked whether a digital identity system would improve the issue of ID theft and fraud in the country (Figure 14) and, below, the effectiveness of the perceived capabilities of the Smart ID card in fighting fraud (Figure 15).

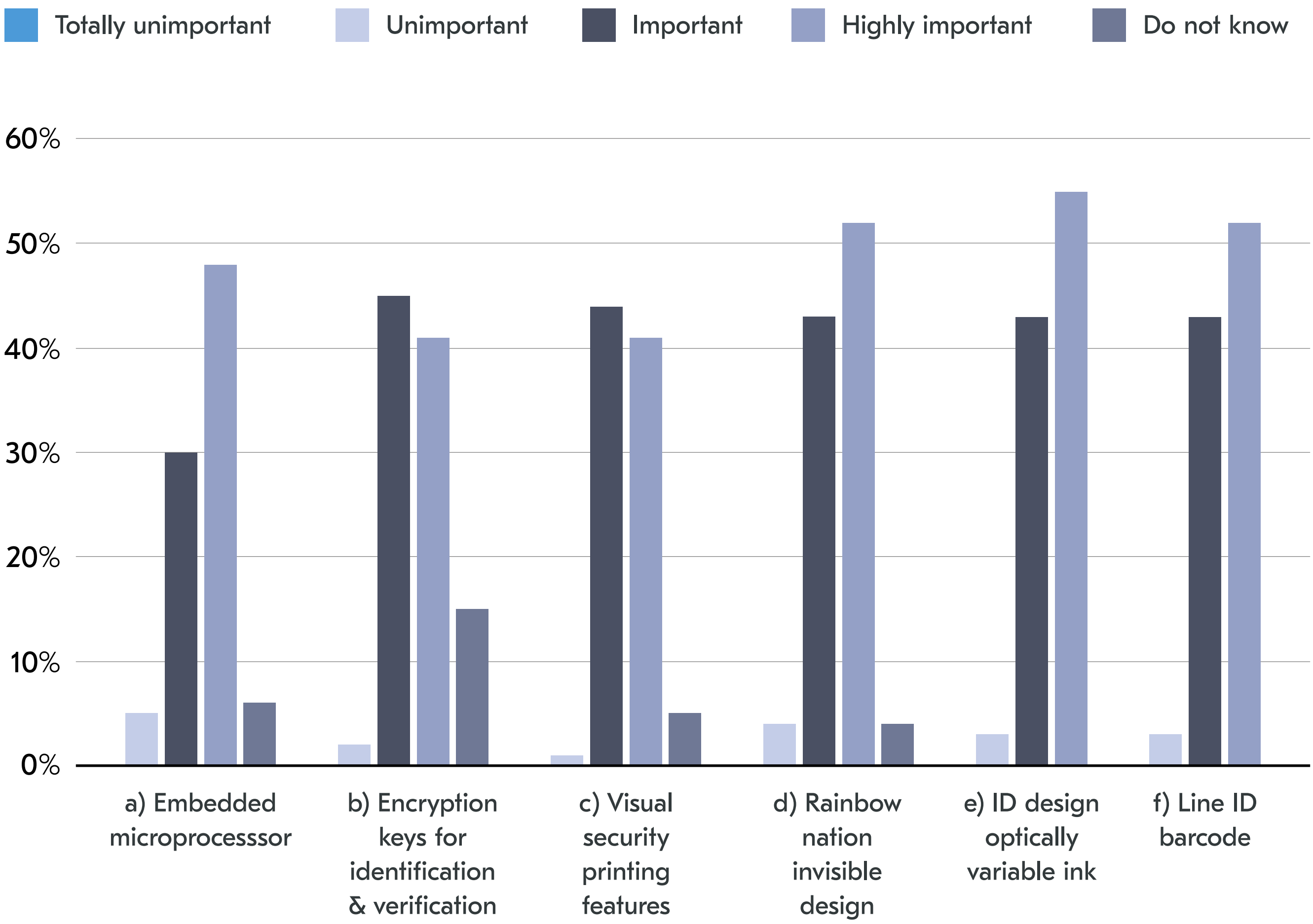


Figure 15: The capabilities of the Smart ID card features

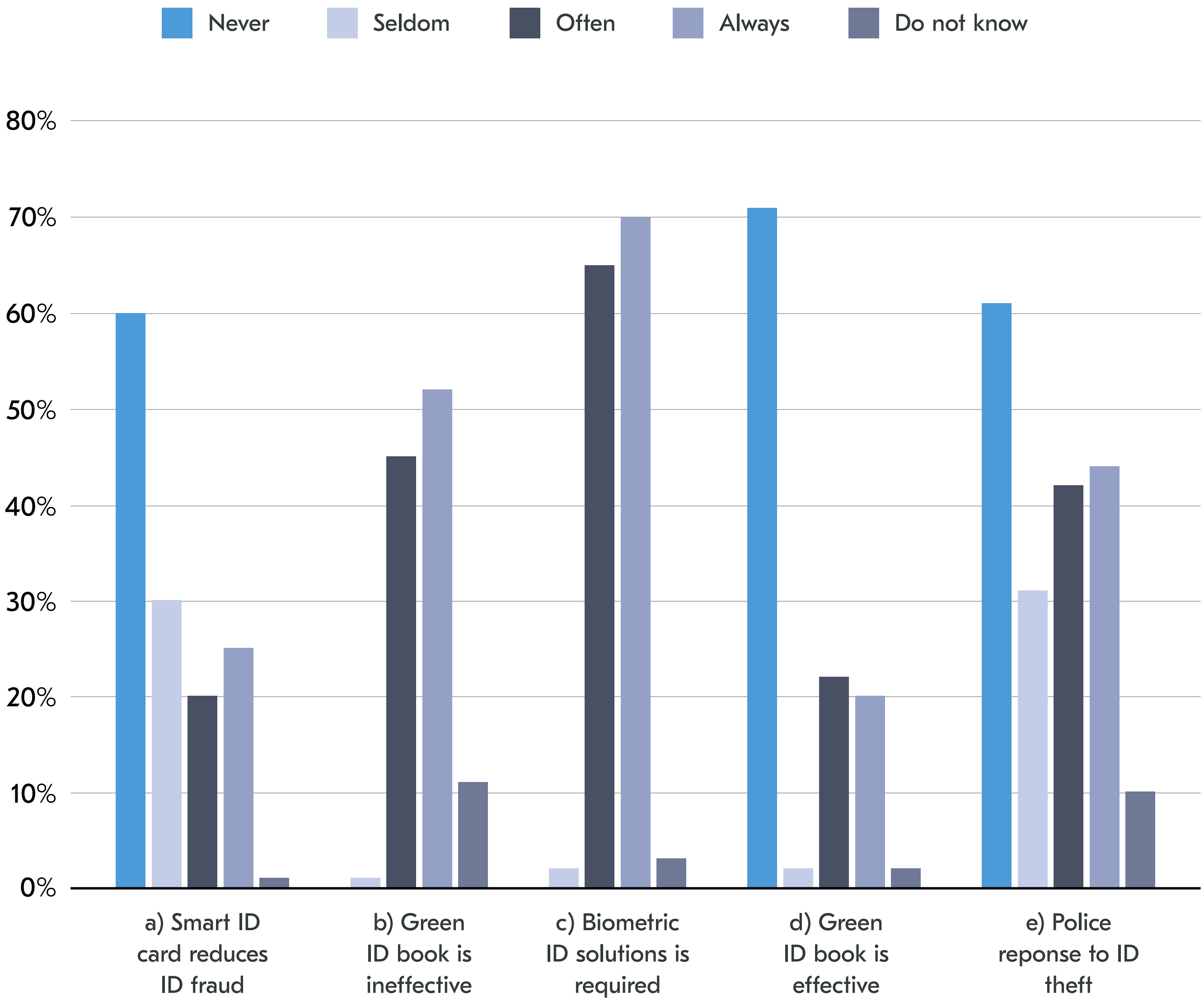


Figure 16: ID fraud trends comparison

Figure 16 summarises the data collected relating to a comparison between the green ID book and the Smart ID card, and also to the need for biometric ID solutions.

5. Discussion of Findings

Identity theft in South Africa is unquestionably an enormous challenge. Nearly half of the country's consumers have either been victims of identity theft or know a person who has been a victim. The major challenge is that the victims only find out about the theft of their identity after several months. Identity theft has increased in prevalence during the COVID-19 pandemic. Since the government has not yet phased out the green ID book, South Africans do not see the need to change over to a Smart ID card. In most rural parts of South Africa there is an increase in reported loss of IDs during exam seasons, and this raises the question of whether schools use other forms of identification instead of an official ID document. In this study, 85% of the participants indicated that a green ID book's key defect has always been that fraudsters can easily change the photograph and replace it with their own. Unscrupulous individuals can then easily use the manipulated ID book to get loans or credit. They can even commit crimes using the identity details in the stolen ID document.

It is concerning that 70% of the participants in this study indicated that despite the apparent increased security features in the Smart ID card, it has been ineffective in the fight against fraud. Techniques such as phishing and pharming have increasingly become popular among cybercriminals (Scarcella, 2020). Criminals are aware of the technology on the Smart ID cards and continue to bypass the weakest link in the security chain.

Despite introducing the Smart ID card and pushing for everyone to upgrade to this form of ID, South Africa has yet to scrap the old green ID book. As a result, it is possible to use both IDs interchangeably. In many rural areas, older people prefer using their green ID book. In contrast, younger people are more comfortable using their Smart ID card. Increasing numbers of young people will only ever know the digital version of their identity. There is an increase in the number of people within communities who now want to shift to using a Smart ID card, and deployments have already been carried out in several schools, rural centres and community halls to facilitate the process.

A primary concern for DHA officials has been the low adoption rate for Smart ID cards in rural communities. Officials have experienced resistance to switching ID format in these communities and have implicated the cost factor in this resistance, as well as the fact that the green ID book is still legally valid. ID replacement is usually expensive for the unemployed, especially those living in poverty in rural areas. On digital ID, the officials have applauded the advantages, but expressed concern for the lack of infrastructure and smartphones; these officials have indicated that it would be useful if a digital ID system could be both online and offline to cater for all communities.

The criminals usually access private information such as ID numbers, banking and card details, home or postal addresses, telephone numbers, email addresses and signatures through practices that range from basic to sophisticated. Some techniques used include intercepting or diverting bank transactions, getting personal information via social media, hacking into computers or email accounts, theft of ID documents and bank cards out of a purse or wallet, theft of account statements in the post, retrieving confidential mail from the garbage, and telephonic impersonation and encouragement to disclose or update information (Thales, 2020).

Identity fraud can go on for months, even years, before the victim realises what is going on. For instance, a Limpopo-based doctor who was 55 years of age had a successful medical career and a thriving business; he only realised his identity had been compromised when he returned to South Africa after having lived in Canada for a year. In addition, many young individuals regard their IDs as useless and feel no need to rush off to get a replacement if they lose one. This neglect plays into the hands of the fraudsters.

Participants in this research study that worked for government entities indicated that during COVID-19 they had faced challenges offering relief to undocumented refugees. Fraudsters regularly take advantage of such people by selling them fake IDs and passports. Recently, a South African Home Affairs official was arrested on charges related to issuing false birth certificates and passports (Sibanyoni, 2020). The inefficiency of the DHA also poses a risk factor in the ongoing ID fraud.

On the 5th of December 2020, the Home Affairs Minister Mr Aaron Motsoaledi said the Department had 813,343 identified cases of blocked identity documents. These are IDs that are suspicious, fraudulent or duplicate. The total includes 517,249 duplicate IDs for cases where individuals have multiple identity numbers or where two people share the same ID number. There were also 17,747 fraudulent cases of deaths, and 145,619 cases where illegal immigrants had accessed fraudulent IDs. Motsoaledi said it takes the department approximately six to eight weeks to resolve and to complete blocked IDs (Maqhina, 2020).

The inability to differentiate between an authentic and a fake ID has been a significant cause of distress, especially in the commercial sectors. A criminal fraudulently assumes the victims' identity in order to get credit, loans, or other benefits in the victim's name, often piling up a mountain of debt in the process. Despite the Smart ID card's being praised for its sophistication, criminals can still recreate a fake Smart ID card.

This situation is fuelled by the lack of infrastructure development, primarily in rural communities. Most bureaucracy in these communities is paper-based, including the process of applying for a job in most government departments. However, that is slowly changing as more and more services are now rolled out online; for instance, around 60% of all recent tax declarations in South Africa were filed electronically. Clearly, the government is now looking into investing in the digital revolution. Regrettably, the Smart ID card that was poised to be a game-changer lacks the right infrastructure to back up the mandate.

6. Conclusions and Recommendations

The focus of this research was to establish the effectiveness of the new Smart ID card in South Africa as there has been no scientific research into this matter. South Africa is a best-case study for digital identity issues in Africa because of its status as one of Africa's leading economies in the technological segment and because it experiences significant immigration of people from other countries within the continent. Research of this nature could guide best practices and models for other African nations. It is important to remember that, given the rapid development of technology, it is far from settled that the best solution for verifying an individual's identity is a secure and user-friendly digital identity system that requires centralised, biometric-based authentication.

Despite efforts to switch to a Smart ID card, identity theft is a growing problem in South Africa. Cases are reported every week of criminals selling fake IDs, licences, passports, and other forms of identification. The number of people who ignore the fact that they have lost an ID, and never report it to the relevant authorities, adds to the problem. The lack of urgency in reporting ID theft is probably not helped by the scarcity of readily available information on the dangers, and potential impact, of having one's ID document stolen. Education is a crucial part of the solution here.

Considerably more time, effort and resources are required if we are to combat ID fraud in South Africa. While things may take a while before they improve, it is also crucial for the victims of identity theft to remember that the very first thing to do is report the case to the police and obtain a case number. This will assist such victims to navigate through the legal system when dealing with banks and retailers. As a consequence of the pandemic, the government has looked into introducing digital vaccine passports; this has been met with resistance from people worried about their data privacy. South Africans barely trust the government and so will be unlikely to trust a new company that wishes to use their data for a digital ID system. In order for digital ID to function, trust needs to be the first ingredient; that can only happen with an extensive awareness and education campaign on digital identity in order to break existing perceptions.

Firstly: The government, or any digital ID company that wishes to open its operation in South Africa, should seek to increase the level of awareness around the consequences of ID theft and also consult with all affected groups, including rural communities. Some of these communities do not understand why they need to switch to the Smart ID card or even the consequences of losing an ID. Some people do not see the importance of replacing a lost ID and can still function adequately without one by using a driver's licence card or passport instead. Both the Smart ID card and license card are easy to duplicate fraudulently. In addition, there is an increasing need for a digital ID given the rise in e-commerce activities. However, the lack of awareness about digital identity and its benefits will always make South Africa a haven for fraudsters. Fraudsters will continue to create fake replicas of Smart ID cards which makes it critical to promote the use of a secure digital ID system, especially now in the digital age when so many transactions are moving online.

Secondly: The telecommunication industry is vital for a digital ID system to be viable in South Africa. Three things need to happen in this area: the government needs to ensure that Wi-Fi access in remote areas is implemented; network providers need to ensure that the digital ID system is free; and there needs to be an alternative offline system. The private and public sectors need to play key roles in ensuring compliance and usage of the digital ID.

Thirdly: The recent Experian data breach demonstrates how vulnerable our country is to cyberattacks. The government needs to invest significantly in cybersecurity systems and digital identity education. The ability of the SAPS to prevent and investigate cybercrime and identity theft remains a concern and this needs to be supported by introducing new or amended legislation on the issues of identity fraud. Scalable blockchain technology needs to be used to protect government data against cyberattacks. Critics argue that a country's digital identity scheme is not an assurance of better service delivery to the citizens. However, blockchain technology, within digital identity, can also help root out corruption. It could add a layer of protection to records that are exposed to high corruption risks.

Finally: The coronavirus pandemic has shown that digital ID can be vital in assisting the South African government to distribute government services. Given the high number of fraudulent cases of ID duplications and ID theft, digital ID can assist the government to ensure the right resources are given to the right beneficiaries. The roll out of vaccines will present another challenge for South Africa, just as the allocation of hospital and medical resources has during the pandemic. A digital ID could ease misuse and ensure that vaccines are distributed effectively. It could also be used to monitor people who have received vaccinations and avoid any form of duplication such as was experienced during the COVID-19 relief allocation.

In order to solve the issue of ID fraud, the South African government needs to embrace digital ID and look into various mechanisms that will be secure, scalable and offer its citizens privacy, while still being transparent. A Smart ID card may not have solved the challenges as the DHA had hoped, but digital ID promises to close that gap. More work still needs to be done to make the subject known to people and to break existing stereotypes and stigmas. Digital ID will one day be a silver stone to South Africa and across Africa, as more and more companies begin heading in that direction.

7. Value of Study

There is a significant gap in the study of digital ID and Smart cards; there is hardly any research focusing specifically on Smart ID cards, let alone on digital IDs in specific countries or the global south. An insightful study was conducted looking at the implications of not having an identity document and only showed the social imbalances faced by the citizens and further looked on exploratory study on causes of Identity Document Theft in South Africa (Maluleke, 2020). This study is a first of its kind in South Africa; it focuses predominantly on the Smart ID card and digital IDs. Much research is centred around cyberfraud as many crimes have been taking place online; most researchers have thus indicated the importance of digital transformation. They have widely warned that such crime will have significant and severe implications.

Many researchers have also focused on the use of biometric systems. Still, the coronavirus pandemic has shown us that we need to rethink the usage of biometrics, and many companies are now looking for contactless digital IDs. The Smart ID card is the latest innovation from the DHA but has proven not to be 100% effective in reaching its intended aim, which is the reduction of ID fraud. Some policymakers have now ruled that a digital ID is a necessary form of identification, specifically when aiming to take advantage of 4IR, which has benefits such as secure access to both government and private sector services; the current study has supported this claim.

8. Future Studies

Implementing Digital Identity Models in South African Banks: A Protection Against Digital Fraud

South African banks are experiencing an increasing incidence of fraud. According to the South African Banking Risk Information Centre report (SABRIC, 2018), incidents of digital banking crime grew by 75% to 23,466 between 2017 and 2018. A total of R262.8m was lost to digital fraud in 2018, compared with R250.5m in 2017. Digital crime as a category includes digital, mobile and app banking. South Africans lost a total of R129m to online banking fraud in 2018. In such fraud, criminals often use phishing emails that request users to click on an email link.

The frauds involve use of credit cards, fund transfers, and so on. As a protection mechanism, future studies should investigate the relevance or role which can be played by digital ID systems in safeguarding the interests of both banking institutions and customers. Such studies should investigate the frauds which are undertaken by using the digital platforms, as well as the parties involved in conducting these fraudulent activities. Afterwards, a model could be constructed highlighting the potential use of digital ID and its role in protecting against digital fraud. In addition, the model could be tested practically by collecting data from the employees of banks and their prospective customers. Digital identity systems are sorely needed in the commercial sector and it is likely that banks can benefit as well.

Shielding Cyber Theft in E-commerce by Adopting A Digital Identity Model: An Empirical Investigation of Digital Fraud During COVID-19 in South Africa

Cyber theft is a significant concern in e-commerce as it can lead to default in online transactions, fraudulent payments, identity theft, and personal information theft, to name a few. Cybercrime incidents could witness a rise of between 40 and 80% in the coming months and years, as consumers and businesses increasingly transact online due to the impacts of the coronavirus pandemic.

With increased digitisation exposing South Africans to more advanced types of fraudulent activity, preventing and minimising the risk of financial fraud has never been more critical. There is also a credit scam that is gaining momentum across South Africa, whereby fraudsters take advantage of consumers in financial distress by offering them high-value loans. "Under the guise of reputable South African credit providers, these criminals appear to be targeting vulnerable consumers via email, with a loan offer of up to R1 million; the condition is that victims must pay an upfront fee of up to R10 000 or more." (BusinessTech, 2019)

To address the issue, especially in South Africa, future studies should aim to identify the major types of cybertheft. Also, the policies of e-commerce should be examined, along with government policies. The effects of the thefts should be analysed from different perspectives. In addition, a model could be constructed which will help in shielding e-commerce platforms from cyber fraud. The model could highlight the significance of digital ID in reducing cyber scams. The model should be examined in the practical environment. The primary data could be collected, and the targeted population will be the employees or managers of e-commerce businesses. The model will address the issues identified, using the help of technology and digital ID systems.

The study will aim at investigating the scams that are taking place currently in South Africa, and their impacts on different factors. The actions taken by the government will be examined. The study will introduce a model which will be able to identify the scammers and take measures accordingly. This will safeguard people from becoming victims of fraudulent schemes and losing finances. Based on research findings, a recommendation will be made concerning the actions which can be taken by the government in order to protect the interests of South Africa's population.

9. Appendices: Initial Proposal

Topic: The effectiveness of the South African Smart ID card in fighting digital identity fraud

Date: 22 — 05— 2019

Background

Digital Identity is increasingly the focus of policy discussions across several different countries, with several governments proposing or implementing national digital identity programmes, and multilateral institutions making investments. Through these government-administered or coordinated programmes, governments aim to provide a single digital identity to residents (or sometimes only citizens) of a particular nation-state. Many such programmes entail a push to collect, store, and use the biometrics of individuals as the primary means of establishing and authenticating their Identity (Khambule, 2018).

Proponents of centralised national ID programmes, particularly programmes promoting biometric linkage, argue that they bring benefits such as more accurate and efficient delivery of government services, anti-poverty regimes and welfare schemes; that they can reduce corruption or increase inclusion; or can help serve national security interests. Critics have responded by noting that national digital identity schemes may not, in fact, ensure more effective distribution of benefits, better service delivery, or improved governance. At the same time, they raise serious concerns, including concerns about how the programmes are designed or governed; social exclusion; privacy and data protection; and cybersecurity (Kaplan, 2017:55).

For digital identity to be empowering in specific contexts, the technological, legal and policy framework must be built on a foundation of user agency and choice, informed consent, recognition of multiple forms of identity, the space for anonymity, and respect for privacy. Focusing on one centralised, directly administered national identity system prevents the formation and competitive use of multiple forms of identity, a competition that could lead to more efficient and empowering outcomes for users. In fact, some argue that government policy should focus on encouraging the development of a variety of identification and credentialing systems, and instead of insisting on it own issued national identity, governments should accept any card or device that provides sufficient proof of the information required for a transaction (Lele, 2017).

Following research into national eID programs implemented by governments across the world, the Department of Home Affairs opted for an ID system - for its high level of security and advanced data-protection mechanisms. In South Africa, two means of authentication will be used — biometric fingerprint verification and a pin code is known only to the user. An embedded secure software with its microprocessor securely contains identification details. It ensures that only authorised authorities can read and verify the card's data using contactless machine-readable scanners. The inclusion of this biometric identification makes it virtually impossible to duplicate the card. It ensures, for the first time, that citizens can be securely authenticated to their eID document (Lele, 2017).

The primary focus of this research is national digital identity programmes that are, policy schemes that governments directly administer or coordinate, which aim to provide a single "digital identity" to one resident or citizens of a particular state. These digital identities are often comprised of compassionate personal information that serves as the basis of authentication or verification of the person's identity. In many such proposed or current programmes, governments store this type of information in centralised databases.

Research Problem

The Republic of South Africa (RSA), has a population of over 51 million and international borders with six different countries, is a multi-ethnic nation. Citizens and permanent residents aged over 16 are required to have a green barcoded identity book which proof of identification for many official uses such as applying for a driver's license or passport, registering to vote and opening a bank account. However, fraud and theft have made the paper book system increasingly insecure for individuals and the state. As part of a significant national investment in technology modernisation, the DHA put in place a Smart ID card system (Greer, 2017).

This research will examine this type of national digital identity programmes from a human rights perspective, discussing the context for the debate about these initiatives globally and proposing safeguards and policy recommendations for those involved: public officials, lawmakers, representatives from judicial and human rights institutions, technologists, officers of development institutions, and members of the private sector. It includes a specific focus on South Africa, with a launched Smart ID card. The Department of Home Affairs started replacing the green barcoded identity documents (IDs) with Smart ID cards on the 18th of July 2013. The new ID cards have better security features and will be extremely difficult to forge. Security features. The has been however many reported cases of fraudulent activities such as identity scams and faked marriages (Li, 2017)

The South African government stated that the card body is secure and durable, made of quality polycarbonate materials which will prevent tampering. It also has two forms of security features: The first is physical security features on the card body such as holograms, laser engraving and personal details which will provide visual verification of the card and quickly identify tampered cards (Kamble, 2018:55). Logical security features include fingerprint biometrics and biographic data, which is embedded on the 80 kilobytes card chip. Personalisation with laser engraving of demographic details and photographs makes the new card extremely difficult to forge or tamper with. The Smart card is believed to cut down on the fraudulent use of fake or stolen IDs, which is a significant concern. Finally, in a separate section, the research will discuss special considerations and recommendations related to introducing biometric IDs, whether in government programmes or private sector (Hanvey, 2018).

Research question

How effective is the South African Smart ID card in fighting digital identity fraud?

1. Have fraudulent activities declined since introducing the Smart ID card in South Africa?

2. What can new development technologies be embedded in the Smart ID card to further secure and protect the digital identity?

3. How can the Smart ID card be utilised to improve future e-government services to citizens?

Aim

The study's purpose is to determine the effectiveness of the launched South African Smart ID card in fighting digital identity fraud. Since its inception, many cases have been reported that comprise fraudulent marriages and identity theft, but the South African Government has remained resilient that this Smart ID card is incorruptible and claims it could only be cases led by the past green bar codded ID. This study wants to uncover all aspects of the Smart ID card features believed to be essential to fight identity fraud, and the study will also make further recommendations to the Smart ID card system to point further in the right digital identity direction and to assist with the national crisis of identity fraud.

Method

A quantitative research method was used in which the primary method of data collection has been adopted. With respect to this, the data collection instrument chosen for the research is in the form of a questionnaire online survey which was sent to the respondents through SurveyMonkey. The sample size for this research was 500 research participants, and amongst these total 500 research participants were head of states, public department managers, citizens including victims of fraudulent activities and industry experts in the Southern Africa region, with the core focus being the Government of South Africa.

Conclusion

The focus of this research was to uncover the effectiveness of this new Smart ID card since there has no scientific research that was done in South Africa that details and focus on this matter. South Africa is a best-case study for digital identity issues, due to its prospects as one of Africa's leading economies in the technological segment as well. A study of this nature, depending on how its outcomes is interpreted, can serve as best practices and models for other African nations. It is important to remember that given the development of technology, it is far from settled that the best solution for verifying an individual's identity is national digital identity systems that require centralised, biometric-based authentication. For example, some scholars propose the use of blockchain technologies to authenticate a user's identity. Since the data stored on the public chain is complicated to change, a user need not provide biometric or other types of personal information to authenticate identity. Therefore, the study aimed to understand the national digital identity crisis and how it can also be addressed by the latest digital technologies that can be merged into the existing Smart ID card to make it more incorruptible to fraudulent activities.

References

Aron, H. (2020). Middle-aged woman leaves hospital 'owning' R2m supercar after ID theft.

https://www.timeslive.co.za/news/south-africa/2020-06-29-middle-aged-woman-leaves-hospital-owning-r2m-supercar-after-id-theft/

Ayanda, K. (2019). Identity is the new gold - and criminals know it.

https://www.bizcommunity.com/Article/196/661/197580.html

Azhar, S. (2017). The fourth industrial revolution and labour: a Marxian theory of digital production.

Review of Socio-Economic Perspectives, 2(1), pp 103–114.

BusinessTech. (2019a). Significant increase in identity fraud cases in South Africa.

https://businesstech.co.za/news/technology/342057/big-increase-in-identity-fraud-cases-in-south-africa/

BusinessTech. (2019b). How to check if your identity has been stolen.

https://businesstech.co.za/news/business/324807/how-to-check-if-your-identity-has-been-stolen/

Cape Business News. (Nov 18, 2020). Identity fraud costs SA over R1 billion during Covid-19.

https://www.cbn.co.za/featured/identity-fraud-costs-sa-over-r1-billion-during-covid-19/#:~:text=ACCORDING%20to%20a%20recent%20local,with%20the%20correct%20ID%20authentication

Creswell, J.W. and Creswell, J.D., 2017.

Research design: Qualitative, quantitative, and mixed methods approach. Sage publications.

Fatorachian, H., & Kazemi, H. (2018). A critical investigation of Industry 4.0 in manufacturing: theoretical operationalisation framework.

Production Planning & Control, 29(8), pp. 633–644. https://doi.org/10.1080/09537287.2018.1424960

Geissbauer, R., Vedso, J., & Schrauf, S. (2017).

Industry 4.0: Building the digital enterprise. PWC.

Hanvey, C. (2018). Data Collection Methods.

In Wage and Hour Law (pp. 19–46). Springer.

Jenna D. (2020). Ukheshe joins forces with Mastercard and Nedbank in South Africa - IT News Africa

Up to date technology news, IT news, Digital news, Telecom news, Mobile news, Gadgets news, Analysis and Reports. https://www.itnewsafrica.com/2020/08/ukheshe-joins-forces-with-mastercard-and-nedbank-in-south-africa/

Jonisayi, M. (2020). 4000 UIF Covid-19 relief claims submitted for dead workers.

https://www.iol.co.za/news/politics/4000-uif-covid-19-relief-claims-submitted-for-dead-workers-df0649f0-1a1f-4ade-ae7a-6052cf52753c

Junie, S. (2019). Identity fraud and theft on the rise in South Africa compared to 2018.

https://www.thesouthafrican.com/news/finance/increase-identity-fraud-and-theft-in-south-africa/

Kabous, R. (2019). How to never ever fall prey to ID theft... and info about a free service if you do.

http://www.702.co.za/articles/304647/how-to-never-ever-fall-prey-to-id-theft-and-info-about-a-free-service-if-you-do

Kamble, S.S. (2018). Sustainable Industry 4.0 framework: A systematic literature review identifying the current trends and future perspectives.

Process Safety and Environmental Protection, 117, pp. 408–425.

Khambule, I. (2018). The role of local economic development agencies in South Africa's developmental state ambitions.

Local Economy: The Journal of the Local Economy Policy Unit, 33(3), pp. 287–306.

Lele, U. (2017). The fourth industrial revolution, agricultural innovation, and implications for public policy and investments: a case of India.

Agricultural Economics, 48(S1), pp. 87–100.

Lesego, M. (2018). The new system detects identity thieves before they drop you into bankruptcy.

https://www.iol.co.za/sundayindependent/news/new-system-detects-identity-thieves-before-they-drop-you-into-bankruptcy-16407554

Maqhina, M. (2020). Home Affairs probes avalanche of blocked ID documents. Independent Online.

https://www.iol.co.za/news/politics/home-affairs-probes-avalanche-of-blocked-id-documents-120e96d4-716f-41f7-bc72-3b03ef02e0d1

Patience, B. (2019) Boxer in ID theft wrangle.

https://www.sowetanlive.co.za/sport/boxing/2019-08-20-boxer-in-id-theft-wrangle/

Rakololo, W., & Maluleke, W., (2020). An Exploratory Study on Causes of Identity Document Theft in South Africa.

International Journal of Criminology and Sociology. 9. 670-685. 10.6000/1929-4409.2020.09.64.

SABRIC. (2018). SABRIC annual crime stats 2018. SABRIC.

https://www.sabric.co.za/media-and-news/press-releases/sabric-annual-crime-stats-2018/

Saunders, M., Lewis, P. and Thornhill, A., 2009.

Research methods for business students. Pearson education.

Saunders, M.N., and Lewis, P., 2012.

Researching business & management: An essential guide to planning your project. Pearson education.

Scarcella, M. (2020). Phishing schemes top COVID-19 digital frauds, TransUnion Survey Says. Credit Union Times.

https://www.cutimes.com/2020/07/24/phishing-schemes-top-covid-19-digital-frauds-transunion-survey-says/?slreturn=20200720051214

Sibanyoni, M. (2020). Home affairs official arrested for 'selling birth certificates'. Sowetan Live, 28 August, 2020.

https://www.sowetanlive.co.za/news/south-africa/2020-08-28-home-affairs-official-arrested-for-selling-birth-certificates/

South Coast Herald. (2020). Beware: Identity theft can land you in boiling water.

https://southcoastherald.co.za/195874/identity-theft-primary-contributor-to-fraud/

Statistics South Africa. (2012). Census 2011 – Statistical release. Statistics South Africa.

https://www.statssa.gov.za/publications/P03014/P030142011.pdf

Thales (2020). South African ID Card - Securing government services.

https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/customer-cases/south-africa

Thompson, A. (2020). The definitive guide to what to do if you lost your ID, passport, credit card or cell phone.

https://www.businessinsider.co.za/how-to-get-your-id-passport-credit-card-cellphone-2020-1

TransUnion (2020). Digital COVID-19 scams focus on ID theft. Security Document News.

http://www.securitydocumentworld.com/article-details/i/16465/

Willemse, I. 2009. Statistical methods and calculations skills.

3rd ed. Juta Lansdowne.

The Yoti Fellowship Programme is one of the key pillars of our Social Purpose Strategy and offers a year long, funded scholarship for people passionate about carrying out grassroots research on identity.

The Fellow's activities can be anything from a technical platform, a report, a website, a book, a policy paper, a film or any other medium relevant to their proposal.

Further details on our Social Purpose Programme, and the Fellowship, can be found at www.yoti.com/social-purpose.