Biometrics as an Agent to Reduce Fraud in the Micro Lending Industry in South Africa

Craven A, Eloff MM

School of Computing

University of South Africa, P. O. Box 392, UNISA, South Africa, 0003

mail: alain@alain.co.za, Eloffmm@unisa.ac.za

Abstract—**We investigate the occurrence of fraud in the micro lending industry and present a pilot biometrics project conducted in Rustenburg with a small group of micro lenders. While similar studies of biometric systems in other countries and industries have been conducted, this paper presents our findings related to the perception of biometric authentication within the South African micro lending industry, and we further present findings related to client resistance in South Africa, both within the micro lending industry, and the population at large.**

South Africa has a large micro lending industry with 3202 registered micro lenders. In contrast there are only 25 registered commercial banks [1]. The smaller lenders are vulnerable to fraud as they are often seen as being "softer targets" and having less secure authentication processes. Internal fraud is committed by staff members who fraudulently issue loans to themselves under assumed names. External fraud is another area of concern, with falsified identity documents and payslips being two of the major problem areas. Biometrics, such as fingerprint readers, have been successfully piloted in a project in Rustenburg, North West Province, to combat internal fraud as well as reduce external fraud. The project will be officially made available to micro lenders in the third quarter of 2010.

Keywords: Biometric authentication, internal fraud, external fraud, micro lending, loans

I. INTRODUCTION

South Africa has a large micro lending industry with 3202 registered micro lenders. In contrast there are only 25 registered commercial banks [1].The smaller lenders are vulnerable to fraud as they are often seen as being "softer targets" with less secure authentication processes. Larger lenders, of which South Africa's major banks form a large part, make use of more sophisticated technology and processes to combat fraud, including mechanisms such as depositing loan funds directly into a bank account, while the smaller lenders often disburse loans as cash.

We have investigated the micro lending industry in South Africa and interviewed leading players in the industry to identify key problem areas. Amongst these areas, the prevalence of identity fraud is a major concern, and has been mentioned by a number of our interviewees.

South Africa makes use of an Identity Number for each citizen, commonly referred to simply as an "ID Number". This ID Number, which consists of 13 numerics, contains a great deal of semantic content:

The first 6 characters are the Date of Birth of the individual in YYMMDD format – the century is not included. Someone born on 4 January 1980, will therefore have the first six digits being: 800104.

The next digit indicates the gender. Numbers 0-4 inclusive for females, and 5-9 inclusive for males.

The next three digits are the sequence number of birth registrations for that day and that gender. The 800th male registered on 04 January 1980 will then have ID number beginning: 8001045800[1]. Historically, the last three digits indicated racial groupings, but this has been deprecated since 1990. The third and second to last digits are now always "08" and the last digit is used for a Check Digit Validation (CDV) calculation. This calculation is freely available from the Department of Home Affairs.

To return to our running example, and assuming the CDV digit is "8", the complete Id number is 8001045800088.

Because of the heavy weighting toward semantic content, and the ease of acquiring the rules governing the CDV number, it is therefore a simple process to "create" an ID Number (as was done in the example). One simply needs to ensure the sequence number is high enough not to overlap with an existing person, and that the CDV is correct. Even if the CDV routine is not available, the ID Number can still be created, and appear to be legitimate. The problem is exacerbated by the fact that credit granters often rely on credit bureaus to determine the authenticity of the ID Number. If a credit bureau does not have the ID Number on file, it will simply report that no match was found and only request the information from the Department of Home Affairs (DHA) at a later stage, in batch mode. Fraudulent ID Numbers therefore appear to have no credit history, which is not traditionally a concern in the micro

1 The 1000th male would be 6000. This very rarely happens, as the birth rate is not sufficiently high.

lending space, as the market was often termed to be "the unbanked", that is, people with no credit history, or access to "formal" financial instruments. However, with increased regulation this has started to change, and the credit history of more individuals is now available.

Fraudulent ID books fall into two main areas:

1) Modified ID Books where a legitimately issued ID Book is modified by changing a combination of the photograph, ID Number and name details.

2) ID books issued via legitimate organisation, but which have been fraudulently acquired. This category may or may not take place with the complicity of civil servants, and civil servants have been arrested for this in the past [2].

Since the ID Books do not contain any special encoding, computer chips, holograms or other security measures, sophisticated equipment is not required to modify them [3].

In our research, we have identified a small pilot project conducted in Rustenburg, North West Province, on the use of biometrics; specifically fingerprints, conducted by a software development company LoanInfo who specialise in systems for micro lenders. We interviewed the owner of the company who sponsored the pilot project and obtained his views.

The remainder of this paper is divided as follows. Section II provides a brief overview of biometrics, followed by Section III which describes the research process and data generation methods. Section IV introduces the micro lending industry and gives a brief overview of the industry and its history, and we follow this with Section V which details the types of fraud and their prevalence. Section VI discusses the acceptance of biometrics in general and in the next section we provide the qualitative results from the pilot study in the micro lending market. We conclude with future research objectives, and a summary of our findings.

The interviewees all commented on the high level of acceptance to the use of biometrics in the micro lending industry and we compare this to informal discussions on the use of biometrics from a South African internet discussion group, international journal articles on the subject and newspaper and other web based articles.

We conclude with an overview of the future research needed in this area, and a brief discussion of the future projects that we are aware of for the micro lending industry.

II. BIOMETRICS IN BRIEF

Authentication can be done by using something the user **knows**, e.g. a password, something the user **has**, e.g. a token or smart card, or a physical **characteristic** of the user, e.g. his fingerprint [4]. Physiological biometrics allows for methods to recognise humans uniquely based on their body. Some examples are fingerprints, face recognition, DNA, hand and palm geometry, iris recognition (which has largely replaced retina), and odour recognition.

Biometrics have found applications in identity management and access control [5], authentication [6], key generation and encryption [7] and even in copyright protection and proof of ownership [8]. Our main focus is the use of fingerprint biometrics for user authentication when approving loans.

Biometric systems operate in either identification mode or verification mode [9]. In identification mode, the person being validated first uses a token that uniquely identifies that person, and then the biometric data is compared to the stored biometric signature. In this way, the token is used to retrieve the stored biometric data from the database.

In verification mode, the biometric data is sampled, and then compared to all the data on the database, with no use of a token to limit the selection size.

III. RESEARCH PROCESS AND DATA GENERATION METHODS

The questions we wanted to answer were:

- Does the introduction of a biometric authentication system to the micro lending industry offer tangible benefits in the combating of fraud, and what is the associated customer resistance?
- What are the perceptions of the micro lending industry in relation to biometric systems?

Data was generated through a series of interviews with leading figures in the micro lending and broader financial arena, as well as leading figures in the fraud prevention industry. Data generation was primarily qualitative, and where appropriate and available, reinforced with quantitative statistics provided by the interviewees and drawn from industry reports. In the case of data drawn from the interview process, all interviewees were given the opportunity to verify the relevant statements, although not all interviewees availed themselves of the opportunity.

Where we were granted permission to use the names or company names of the interviewees, we have done so. Not all individuals and / or companies wanted to be named.

We conducted interviews with companies involved in the provision of biometric systems, fraud prevention, software development, micro lending, banking, industry regulations and credit bureaus.

In order to establish the types of fraud prevalent in the credit market overall, and the perceptions of companies in relation to fraud we conducted face to face interviews with the Executive Director of the South African Fraud Prevention Service.

We interviewed the Managing Director of a leading biometric company, which specialises in fingerprint biometric technology, and works closely with the private sector as well as with

governmental departments. They were able to provide us with a qualitative analysis of the general perceptions pertaining to fingerprint biometrics in the industry, as well as invaluable background information in terms of the technology and available systems.

To understand the micro lending perceptions of biometrics, as well as to gain insight into the pilot project conducted in Rustenburg, we interviewed the founder and Managing Director of LoanInfo, who developed the software system that incorporates the biometric system.

Our last interviewee was the Managing Director of Consumer Profile Bureau, South Africa's second oldest credit bureau, who provided us with background information to the micro lending industry.

In order to answer the research questions, both the real and perceived benefits of using the system, and the costs (both tangible and intangible) of using the system had to be taken into consideration. However, with the exception of the SAFPS, no central organisation actively collects data related to fraudulent activity. If a loan is fraudulently disbursed against an individual, that loan is simply deleted from the credit bureaus, and no aggregated totals of these are collected. As such, it is difficult to obtain an industry average of fraudulent loan disbursement, especially with the restrictions placed on SAFPS in regards to data sharing; however in 2002 the loss to the banking industry alone was estimated to be R4 billion rand [3]. It is estimated that identity theft alone causes a R1 billion annual loss, but "nobody has got any real figures" although Alexander Forbes estimated the quarterly loss at the time to be R276 million. [10]. In the United States, identity theft is estimated to have cost $49.3 billion in 2007 [11]. The South African credit industry disbursed approximately R47.5 billion [2] for the third quarter of 2009, of which approximately R9.5 billion rand was unsecured and short term loans. 44% of all credit applications are rejected for various reasons [1], some of these are assumed to be rejected as a result of fraud, but no aggregated statistics are publicly available [1].

The system costs were examined along two dimensions, perceived loss of customers due to the introduction of the system, and the actual cost of the hardware and software, and associated training. The perceived loss of customers is a qualitative perception and care needs to be taken in extrapolating this figure to the general population, for two reasons:

1: the loss of customers needs to be balanced against a reduction of fraudulent activity; less customers applying for credit may be a factor of the improved security and the criminal's perception of the business no longer being a “soft target”.

2: the credit industry has been in a recession, with credit granting down 25.71% year on year from quarter 3 of 2008 to quarter 3 of 2009. In addition, the number of credit applications received by the credit industry has dropped by 7.77% year on year, with the total book value of short term, unsecured, credit transactions having declined 15.04% for the same period. In terms of risk exposure, the smaller loans in terms of loan value have shown a sharp drop of 37.43% for loans under R3 000, and an increase in loans over R15 000 of 16.84% [12].

The costs of Biometric Equipment varies as does the expense relative to an organisation's income and expenses. We therefore concentrated our attention on the perceived costs and the willingness of the organisations to incur these costs.

IV. Background Of The Micro Lending Industry In South Africa

In order to present our findings and research in context, and to convey the perceptions and fears of the micro lending industry towards increased technology it is important to look at the history of the industry.

The South African Micro Lending industry has been in existence for many years[3], and until relatively recently was unregulated. The Usury Act Exemption Notice of 1999, and the subsequent founding of the Micro Finance Regulatory Council (MFRC) paved the way for more stringent credit control policies, culminating in the National Credit Act 34 of 2005. Increased regulations also brought with it the need for increased technology, and a more stringent control of the accounting practices and corporate good governance. Prior to regulation, many lenders operated their businesses with paper files, but increased regulation prompted the need for computer systems and Internet access.

With the Usury Act Exemption Notice, larger lending organisations were enticed to enter the micro lending industry, including the major commercial banks. Although there was no regulation preventing them from doing so before that, they were constrained in the interest rate charges to that allowed by the Usury Act. Despite this new entrant, the SME micro lenders continued to grant loans, primarily as a result of the large institutions not having the same risk appetite. The micro lending industry in South Africa operates at relatively small profit margins, and high risk due to the lack of loan security (collateral).

When small micro lenders registered with the MFRC many of them did not have the equipment that large commercial banks would consider as a minimum requirement. These included fax machines, computers and dedicated telecommunication lines and computer modems. This led to initial difficulties in performing basic verification of consumer details and credit history, and created an environment that existed without the need for technology. Different technologies were however introduced to assist them, including basic credit checks performed on an audio-text system, and call centres.

2 At the time of writing, the South African Rand was trading at approximately R7.50 to the USD.

3 It is generally agreed that the modern industry found its roots in the farming communities of Potgietersrus in Limpopo during the early 1990s. However, moneylenders have been in existence for centuries, with historical references of micro lending activities dating back at least to Roman times.

Because micro loans are commonly unsecured loans, and the market that is being served is often migratory or without a fixed residence or place of employment, micro lenders used to hold the borrower's ID Book and bank ATM card for the duration of the loan. In many cases, the lender used to withdraw the loan payment directly from the borrower's bank account before returning the card and ID book, and in this way a limited form of securitization was achieved. With the regulation of the industry, the South African government made this practice illegal [13], and it is a criminal offence under Section 133 of the National Credit Act (NCA) 35 of 2005 [14], and some lenders have been arrested for contravention [15].

When the MFRC introduced the National Loans Register, and later with the introduction of the NCA, lenders were compelled to perform credit checks on clients and register their loans on a central database[4]. This led to an uptake of technology (particularly computers and modems) in the industry, but even to this day a sense of technophobia is prevalent.

It is against this backdrop and history of increasing reliance on technology, a reduction in loan security, and increasing visibility and regulation of the industry, that the introduction of biometrics is being made.

V. Fraud Statistics And Preventative Measures

We conducted face to face interviews and email interviews with key figures in the credit bureau industry, the financial lending industry, as well as the fraud prevention industry to identify the prevalence of fraud, and the main categories of fraudulent activity.

We interviewed the executive director of the South African Fraud Prevention Service (SAFPS, http://safps.org.za/), South Africa's leading provider of fraud prevention data, who provided us with an overview of fraud statistics. The SAFPS is a non-profit organisation with a voluntary membership structure, and has amongst its members major banks and retailers, Confidentiality agreements between the company and its members prohibit the release of exact statistics, but we were provided with a qualitative overview of the industry and broad problem areas.

Amongst the major concerns recorded is the number of fraudulent ID books in South Africa, along with fraudulent use of identification documents. South Africa's ID book is easily forged [3]. The two areas of fraud are not identical, with fraudulent documents being documents that are illegally manufactured and appear to be legitimate, and fraudulent use referring to the passing of a *legitimate* document by someone who is not the legal holder of the document.

SAFPS estimates that 20% of all fraud is conducted with an illegitimate ID book, while 30% of all fraud is conducted through *impersonation,* which is the passing of a legitimate ID book by someone who is not the legal holder of that document.

Another key problem area is internal fraud. Some organisations have little internal security and it is easy for staff to fraudulently issue a loan against a client who has not borrowed for some time, and then pocket the money themselves. This is of particular concern among “cash businesses” where loans are issued in cash, but is of less of a concern where loans are disbursed directly into bank accounts. In our interview with SAFPS, it was stated that many organisations do not actively combat fraud, although they admit to the need for it. In many cases, it is seen as being “too costly” or “taking too long / too much time” to actively combat fraud. The LoanInfo prototype system that we examine later combats this type of fraud by requiring staff members to enrol in the biometric system, and for clients to be biometrically identified at the time of loan disbursement.

The nature of the fraud crimes also often differs, with fraudulent documentation being linked to criminal syndicates, while fraudulent use of documents is linked to criminal syndicates as well as “crimes of opportunity”. The latter fraud is perpetrated by people who happen to be presented with the chance to be dishonest, but are not career criminals. Our interview with SAFPS confirmed how an adult sibling would make use of the identity document of a recently deceased sibling when applying for a loan, and then not repay the loan. When legal action is taken, the person recorded as the borrower is found to be deceased.

Since the SME micro lending industry often only require an identity document and a payslip to issue a loan, it is relatively easy for fraudulent activity to take place. All our interviewees confirmed that micro lenders are targeted by syndicates operating with fraudulent documentation, including payslips. These syndicates are sophisticated, and employ people to operate in mini-call centres that masquerade as the human resource department of large organisations. Lenders will call the telephone number on a payslip, and be under the impression that they are speaking to the human resources department of a large corporation, and then proceed to verify the employment details. SAFPS commented that it is relatively easy to purchase a fraudulent payslip, from as little as R200, while in our interview with LoanInfo it was stated that a false ID book, three months fraudulent bank statements, a fraudulent payslip and a fraudulent bank card could be purchased for as little as R60.

In our interview with companies supplying biometric equipment and services, the primary reason given for the reluctance of micro lenders to exercise better security measures is that the cost of formal security systems and vetting of applications is simply not feasible with the small loan amounts (and associated profit). This was confirmed by LoanInfo who conducted the pilot project in Rustenburg. Both interviewees however did state that the micro lenders saw value in the process itself and

4 Neither of these are explicitly included in the National Credit Act, which supersedes the National Loans Register. Credit granters are however compelled to ensure clients can afford repayments – although the mechanism to ensure this is not stated. In addition, provision has been made for a National Register of Credit Agreements, which will hold all credit obligations, but this has, to date, not been completed.

were keen to be involved, but were restricted by costs.

Typically the micro lending business needs to perform at least a Credit Check on a client to ensure affordability. This is mandated by the NCA (National Credit Act 35 of 2005) which specifies that a lender must ensure that the client can afford to make repayments and that his current loan obligations does not exceed his income. These fees can range from R2.50 to R30 for each credit bureaux on which an enquiry is performed. Since loan amount are typically small, and repayment periods can be as little as one week, individual transaction fees for vetting and approving loans is high in terms of the interest charged. Any system that proposes to reduce fraud would also therefore need to be cost-effective.

VI. Resistance To Biometrics In The Formal Sector

Biometric systems in the formal sector show a long history of consumer resistance [16],[4]. Quantitative analysis of responses from an on-line forum (the forum, MyBroadBand.co.za is one of the popular forums in South Africa, with a large population of technical people, as well as a population of people from all fields and areas) over the recent introduction of biometric systems in the formal banking sector of South Africa shows an aggressive attitude towards the system [17]. A qualitative analysis of the results is provided in Table 1. A total of 52 posts were made at the time of the analysis. We omitted posts that did not pertain to the topic at hand, such as “lol” in relation to a previous post.

TABLE 1: Responses To Announcement Of Biometric System In A Large South African Bank.

Keyword or Key Concept	Total occurrences	Percentage of posts
Not Happy, But Accepting	1	2%
Application Scoping	1	2%
Legality	2	4%
Rise in violent crime	2	4.00%
Anger	3	6%
Cost Fears	3	6%
Happy	3	6%
Privacy Concerns	4	8%
Implementation Concerns, as well as belief it will not happen	4	8%
Security Concerns	6	12%
Resistance	7	13%

Internationally, the response to biometric systems has started to see an increase in acceptance. Unisys (www.unisys.com) have conducted research that indicates 56% of UK citizens would be prepared to use biometric verification, and 95% of those would be willing to use fingerprints [18].

In our interview with biometric suppliers, it was stated that South Africans do not have as high a resistance to biometric procedures as some other countries, possibly because citizens have become acculturated to the idea as they are required to supply fingerprints when applying for an identity document, a passport and a driver's licence.

However, it was also stated that there is resistance to biometrics in the workplace by trade unions who have been successful in preventing the use of biometrics for time-tracking. The unions argued from the point of increased risk of infection, and this argument does find support in the literature [19].

Capitec Bank, who use biometric systems to record transactions performed by bank staff, and who make use of photographic identification to identify clients, have been highly successful in the South African Financial arena [20].

Further research in the South African market on the affects of biometric acculturation would be instructive, as would research into people's stated opinions and their real world behaviour.

VII. Results Of Pilot Study

Participant Selection for the Pilot Stage

The pilot study that forms the basis of this research was conducted by a software developer specialising in the provision of software products to the micro lending industry. The participants involved in the pilot study were chosen based on their relationship and geographical proximity with LoanInfo, the software development company. The participants therefore represent a small subsection of the entire population, and the experiences and perceptions of this sample group and their clients may not be transferable to the population as a whole. A total of six companies participated in the pilot phase. Unfortunately the pilot study was already under way at the time of this research paper being written, so it was not possible to conduct a pre-pilot survey of the micro lenders. It is envisaged that this research will be conducted before the release of the full system to a wider target group.

Overview of the current system

The pilot project makes use of the identification mode for all transactions, and requires an initial enrolment phase to store the biometric data on the database.

The pilot study was incorporated as part of an existing administration system for micro lenders. This system offers client maintenance, loan maintenance, payment routines and integration into credit bureaus, fraud prevention databases and closed user group (CUG) databases. Among these CUGs is a

fingerprint biometric database. The system allows businesses to record the fingerprints of their staff members as well as their clients and prospective clients, allowing organisations to ensure that loans can only be disbursed on successful verification of a pre-recorded fingerprint, and to prevent loans being disbursed to staff members without supervisor authorisation (along with another fingerprint authentication). Payments are also recorded by means of a fingerprint, with both the client and the staff member supplying this biometric information. No additional licensing fee or purchase cost was applied to the software package, and each micro lending company purchased their own fingerprint scanner.

The enrolment phase presents the weakest point in the security system, as false enrolment will result in subsequent false identification. Personal information of new clients is loaded onto the database, and their fingerprints are scanned and loaded to the central database. While consideration is being given on providing organisations with access to the biometric data held by the Department of Home Affairs, proposed legislation, such as PoPI (discussed in the next paragraph) makes this difficult; however commercial banks in South Africa have been allowed access [21], so the possibility of expanding this to other lenders may exist.

The Protection of Personal Information Act (alternatively PPI or PoPI), which at the time of writing is still a draft bill that has not been promulgated, legislates, amongst other things, the storing and sharing of biometric information [22],[23]. PoPI is due to be promulgated at the end of May 2010.

Early indications are that information such as biometrics will require that consumers provide informed consent before the information can be distributed. This is not a barrier to a system that collects new biometric information, as informed consent can be obtained at the enrolment stage, but may make it more difficult for organisations to retroactively acquire existing data.

In our interview with LoanInfo, it was stated that the pilot test did not negatively affect the volume of loan registrations, and one of the companies involved in the project reported “no resistance at all”.

VIII. Call To Arms And Future Research Objectives

The initial studies conducted have shown that the perceived value of the biometric system in the SME micro lending industry is positive. Client resistance is also lower than in other market sectors, and appears to be lower than international norms.

Future research will need to be conducted to evaluate biometric systems in a larger population, and with more rigid, quantitative analysis of the true costs and benefits.

Currently, the pilot project has been suspended, and an improved system is being completed for implementation in the third quarter of 2010. The improved system has incorporated suggestions based on discussions with the pilot users. Additional features have been incorporated, such as the ability to record fraudulent activity for future research purposes and to measure changes in this activity. It is hoped that this system will be able to answer some of the unanswered questions, namely:

- Is there a quantitative basis for saying that biometric systems reduce levels of fraud?
- Is there a quantitative basis for saying that the micro lending client base does not view biometrics in a resistive manner?
- Does a biometric system offer users and clients a better user experience, and does it help eliminate bottlenecks on busy days?
- Is it possible to build a reliable, useful and accessible database of micro lending clients to assist in reducing paperwork, and enhancing the credit enquiry process?

In addition, active tracking of fraudulent loan disbursements will be introduced, and this will allow us to track changes in fraud prevalence within the industry for those lenders making use of biometrics.

IX. Conclusion

When biometrics were first introduced to the micro lending market, resistance from business owners was high. The initial cost of the system was deemed to be too expensive, and there was little perceived value.

The pilot project, and other recent investigations by the companies we interviewed, has shown that the perception of value has been changed, and that the resistance from clients (borrowers) is not nearly as high as initially suspected. Within the more formalised micro lending environment, the introduction of various biometric identification systems has not led to consumer resistance, and companies such as Capitec have in fact increased market share.

In today's tough economic times and with increasing regulation that prohibits and punishes the withholding of client's ID documents and bank cards as security, the biometric system now represents a smaller investment cost in terms of the higher risk of lending money, which is supported by the particular fraud areas identified by SAFPS that pertain to the micro lending industry, and it is hoped that the system will continue to offer real value to its users.

Future research will be conducted to collect quantitative data from micro lenders on fraudulent loan activity, and a comparison will be made between the rate of fraudulent loans and the adoption of biometric systems.

REFERENCES

1. Tlakula P. *National Credit Regulator Annual Report 2008 / 2009*. National Credit Regulator; 2009. Available at: http://www.ncr.org.za/pdfs/ANR2009/NCR%20REPORT%202009.pdf [Accessed May 7, 2009].

2. McCarthy S. South African Department of Home Affairs. Home Affairs Officials Arrested. 2008. Available at: http://www.home-affairs.gov.za/media_releases.asp?id=496 [Accessed May 8, 2010].

3. Reid J. SA ID book 'one of the easiest in world' to forge - Hi-Tech Security Solutions. 2003. Available at: http://securitysa.com/news.aspx?pklNewsId=9941&pklCategoryID=106 [Accessed May 7, 2010].

4. Pfleeger, Pfleeger. *Security in Computing*. Fourth Edition. Prentice Hall; 2007.

5. Edwards MB, Torrens GE, Bhamra TA. The use of fingerprint contact area for biometric identification. In: LNCS 3, ed. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer Berlin / Heidelberg; 2006:341-347.

6. Xiang W, Desai B, Wen P, Wang Y, Peng T. A Prototype Biometric Security Authentication System Based upon Fingerprint Recognition. In: *RSKT '09: Proceedings of the 4th International Conference on Rough Sets and Knowledge Technology*. Berlin, Heidelberg: Springer-Verlag; 2009:264-272.

7. Han F, Hu J, Yu X. A biometric encryption approach incorporating fingerprint indexing in key generation. 2006. Available at: http://researchbank.rmit.edu.au/view/rmit:3037.

8. Ahmad S, Lu Z. A Joint Biometrics and Watermarking Based Framework for Fingerprinting, Copyright Protection, Proof of Ownership, and Security Applications. In: *CISW '07: Proceedings of the 2007 International Conference on Computational Intelligence and Security Workshops*. Washington, DC, USA: IEEE Computer Society; 2007:676-679.

9. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. *IEEE Trans. on Circuits and Systems for Video Technology*. 2004;14:4-20.

10. Kept. Identity theft costs SA more than R1-billion a year. 2010. Available at: http://inf.cc/kept/index.php?option=com_content&view=article&id=41%3Anewsflash-5&catid=3%3Anewsflash&Itemid=1 [Accessed May 8, 2010].

11. Privacy Rights Clearinghouse. Identity Theft Surveys and Studies: How Many Identity Theft Victims Are There? What Is the Impact on Victims? | Privacy Rights Clearinghouse. 2010. Available at: http://www.privacyrights.org/ar/idtheftsurveys.htm#Jav2007 [Accessed May 4, 2010].

12. Devpruth R. *NCR Consumer Credit Report*. South Africa: National Credit Regulator; 2009. Available at: http://www.ncr.org.za/publications/Consumer%20Credit%20Report/Septem_2009.pdf [Accessed May 6, 2010].

13. Ferreira H. Misconceptions. Available at: http://www.mfsa.net/new/index.php?option=com_content&view=article&id=6&Itemid=6 [Accessed May 8, 2010].

14. NCR. NCR. 2005. Available at: http://www.ncr.org.za/ [Accessed May 7, 2010].

15. Africa F. *NCR intensifies its fight against lenders flouting the National Credit Act*. National Credit Regulator; 2009. Available at: http://www.ncr.org.za/press_release/NCR%20intensifies.pdf [Accessed May 7, 2009].

16. Schuman E. Consumers Resist Retail Biometrics - Enterprise Applications from eWeek. 2006. Available at: http://www.eweek.com/c/a/Enterprise-Applications/Consumers-Resist-Retail-Biometrics/ [Accessed May 4, 2010].

17. MyBroadband. SA Banks to begin to implement online fingerprint verification. *MyBroadband*. 2010. Available at: http://mybroadband.co.za/vb/showthread.php?221383-SA-Banks-to-begin-to-implementonline-fingerprint-verification [Accessed May 4, 2010].

18. Neal D. UK consumers warm to biometrics - 20 Oct 2009 - Computing. 2009. Available at: http://www.computing.co.uk/v3/news/2251595/unisys-releases-security-survey# [Accessed May 4, 2010].

19. Jacobs JA, Ranst MV. Biometric Fingerprinting for Visa Application: Device and Procedure Are Risk Factors for Infection Transmission. *Journal of Travel Medicine*. 2008;15(5):335-343. Available at: http://dx.doi.org/10.1111/j.1708-8305.2008.00232.x.

20. Capitec. Key facts | Investor Centre | Capitec Bank. *Key Facts Investor Centre Capitec Bank*. 2009. Available at: http://www.capitecbank.co.za/ir/about/keyfacts [Accessed May 7, 2010].

21. McCarthy S. South African Department of Home Affairs. BANKING INDUSTRY AGREES MILESTONE ID FRAUD PREVENTION PROJECT WITH HOME AFFAIRS. 2010. Available at: http://www.home-affairs.gov.za/media_releases.asp?id=594 [Accessed May 7, 2010].

22. Money-business. Protection of Personal Information Bill - POPI Act | Money Business. 2010. Available at: http://www.money-business.co.za/business/protection-of-personal-information-bill-popi-act/ [Accessed May 7, 2010].

23. Deloitte. Protection of Personal Information Bill. 2010. Available at: http://www.deloitte.com/view/en_ZA/za/services/za-legal-en/article/9d430a5e9cd27210VgnVCM100000ba42f00aRCRD.htm [Accessed May 7, 2010].