HELP US! WE WANT TO BE 'E-SECURED': DIGITAL BANKING CUSTOMERS' SECURITY NEEDS IN SOUTH AFRICA

Arthur Goldstuck[1], Rabelani Dagada[2]

[1] World Wide Worx,
[2] University of the Witwatersrand

[1] arthurg@internet.org.za,
[2] Rabelani.Dagada@wits.ac.za

ABSTRACT

In the context of this paper digital banking refers to online, mobile, and Automated Teller Machine (ATM) banking. Digital banking, particularly online and mobile banking, is growing rapidly in South Africa. This is happening despite heightened security concerns, created in part by the media. The 2008 World Wide Worx and Wits Business School Digital Banking Research found that the level of sophistication related to the electronic related crime in the banking sector is extraordinary. The aforesaid research revealed that most of the digital banking crime affect online banking and ATM. The media captured the crime phenomenon by using catchy headlines. The 2008 World Wide Worx and Wits Business School Digital Banking Research employed both qualitative research approaches. Quantitative data collection method was employed at an elementary level to capture relevant statistics. Purposive sampling was used to select the participating banks. Researchers deliberately targeted the biggest banks in South Africa - Standard Bank, ABSA, Nedbank, and Investec. Although the First National Bank did not participate in the 2008 study, researchers made deductions based on previous engagement with the bank. The research findings reflect various types of digital banking related crimes and some of the measures taken by the banks. These include SIM [Subscriber Identity Module] swop fraud, phishing, ATM bombings, card swapping, and card skimming.

Seeing that customers are extremely concerned about the digital banking crime, the banks are reacting to the crime swiftly with a lot of sophistication. The phishing websites are removed and suspicious emails blocked. The spoof site can be knocked off the web within 48 hours whilst the fraudsters are tracked down speedily. With the assistance of the South African Police Services, banks have managed to bring down the frequency of the ATM bombings. Some of the methods employed by the banks to combat e-crime are very controversial. For example, some of the banks hire their own hackers and bomb their own ATMs. Banks also have dedicated e-crime units and invest huge financial resources on customer education. These initiatives are yielding good results. In the medium to long term, the success of countermeasures to crime in digital banking increases client confidence. Interestingly, this study found that some banking customers did not have fears regarding mobile banking as a delivery channel.

KEY WORDS

Digital banking crimes, e-security, methods to fight crime, client confidence

1 INTRODUCTION

The Digital Banking in this study refers to the online, mobile banking, and Automated Teller Machines (ATMs). Online Banking refers to the use of the Internet for banking transacting purposes whilst mobile baking is defined as the employment mobile devices such as cell phones to conduct banking activities. According to the 2008 World Wide Worx and Wits Business School Digital Banking Research (Goldstuck and Dagada, 2009), Online and Mobile Banking were launched in South in or around 1996 and 2000 respectively. The subscriber base for Digital Banking in South Africa reached 5719280 mark by December 2008. 3642340 of this number represented the Online Banking users, whilst Mobile Banking customers are 2076940 (Goldstuck and Dagada, 2009). This is a drastic development when one reflects on the 2006 Online Banking Report (Goldstuck, 2006). According to the aforesaid report, "Online Banking reached the one million mark in South Africa for the first time at the end of 2003, grew to 1,4-million in 2004 and 1,7-million in 2005. According to Goldstuck and Dagada (2009), the number of Digital Banking accounts has grown rapidly since 2005. The growth in Digital Banking has been happening despite security concerns by both the bankers and customers.

Other than focusing on the growth of the Digital Banking, the 2008 World Wide Worx and Wits Business School Digital Banking Research paid attention to the factors that affect the adoption of the Digital Banking services. These included the usefulness, ease-of-use, experience of the user, enjoyment, trial-ability, availability of information, self efficacy, and security. These factors were derived from the theories that deal with technology adoption. These include Theory of Reasoned Action (TRA), Technology Acceptance Model (TAM), Theory of Planned Behavior (TPB), and Innovation Diffusion Theory. For the purpose of this paper, authors would mainly focus on security as a factor that affects the adoption of Digital Banking channels.

2 THE CRISIS OF 2003[1]

On 12 May 2003, Katja Hiller-Staal, the manager of the Digteby Guest House in Ridgeworth, a suburb of Bellville in the Western Cape, discovered that R30 000 was missing from her bank account with Absa. She reported the matter to the bank, and then to the police. On 27 June 2003, Helene van Tonder, a bookkeeper from Bellville, visited an ATM to draw money from her account. Her salary of R15 000 had just been paid in. But when she called up her balance, the whole amount had disappeared. Within weeks, these two women would discover they had played a role in the most tense drama in the history of online banking in South Africa. Their losses set in motion a series of events that would first appear to be a lethal blow to the industry, but would culminate in a quiet vote of confidence from the public. Van Tonder also contacted her bank, Absa, who advised her to lay a charge with the police. She was reimbursed but, on being told that somebody had gained access to her account via the Internet, she cancelled her Internet account with the bank. And both the bank and the police drew her into an intensive investigation.

On Sunday, 20 July 2003, the Sunday Times carried the news of South Africa"s first case of money stolen through online banking. According to the report, the Police Commercial Crimes Unit had confirmed that week it was investigating nine cases involving thefts from Absa accounts. It appeared that the perpetrator used "spyware" to gain access to the personal computers of the victims. Internet banking information found on the computers was then used to transfer money out of their accounts. Police had confirmed total losses of R230 000 reported to them, but on Friday 18 July attorney Harry de Villiers found R300 000 had gone missing from one of his trust accounts when he went to check his statements. He said the bank had only alerted him to R10 000 that was transferred into one of his accounts earlier in the week. Absa described the crimes as "identity fraud", which they said had been “committed by a person who had gained access to clients' accounts through their own personal computers using the Internet”. Group information security officer Richard Peasy pointed out that the bank's "security systems and processes

[1] This section has been adopted from the World Wide Worx’s Online Banking Report in South Africa. The research report was composed by Arthur Goldstuck who is the co-author of this paper.

had alerted the bank to suspicious activity before these clients knew about it. The transactions were frozen and the process for dealing with potentially fraudulent transactions was instituted”. However, according to Harry de Villiers, the bank had only alerted him to R10 000 that was mysteriously transferred into one of his accounts earlier in the week. When he checked his accounts more closely later, he discovered that amounts of R227 000 and R93 000 had been transferred to another account. Upon further inquiry, it emerged that the person had bought 15 laptop computers by transferring some of the money into the account of the computer company and the rest into an account at a different bank. Peasy pointed out: "As with other banking channels, no fraud can take place on Internet banking accounts without the fraudster obtaining the client's Internet banking access account number and PIN number." He said it appeared the fraudster had sent unsuspecting clients an e-mail, which, when it was opened, installed software that recorded information. "It is a new trend called spyware. This has got nothing to do with the bank. It records keystrokes, like your account and PIN number, and then it e-mails the information to a Hotmail mailbox."

Absa told Finance24 that it would repay money stolen via the Internet from the accounts of three clients, but only if an investigation by an auditor confirmed that the money had, in fact, disappear in this manner. On Monday, July 21, Banking Council spokeswoman Claire Gerbhardt-Mann announced that hackers could be using home computers to steal money from Absa Bank clients, but that they were not breaking into the systems of the bank itself: "Because they are finding it increasingly difficult to breach the banks' own security systems, they are beginning to turn to weaker links outside of these systems, for example, Internet service providers or the customers' own PCs. "In this specific instance, it appears that the loophole was not in the banks' system but that home computers are being compromised." The Banking Council advised the public to make sure that no one had unauthorised access to their computers, to install the latest anti-virus applications on their computers, exercise control over the shared folders, keep their PIN secret and to never disclose their PIN to anyone, including bank staff. On Tuesday, 22 July, after officials from the four major banks held talks in Johannesburg, Richard Peasey issued the following statement: "We took the initiative in convening the meeting to share information about this new crime with the other banks. Each of the banks will use the information provided to the benefit of their own customers. Absa and the rest of the banking industry have come together to combat this new crime… Our focus is on educating and sharing information to ensure peace of mind for consumers." All four banks issued statements assuring customers of the safety of online banking, with Absa and Standard Bank launching major campaigns to make anti-virus software and firewalls available at no cost, and FNB offering a money-back guarantee. Only Nedcor did not amend its existing strategy, announcing that it had implemented additional security measures a year earlier in anticipation of precisely this kind of fraud. The very next day, ironically, on 23 July, African Bank confirmed that its web site, www.africanbank.co.za , had been hacked into by an unknown party on the Sunday on which the online banking fraud was first revealed. However, no permanent damage had been done, with only the home page defaced. It was replaced within a few hours.

Finance24 reported that the site, which was purely for information purposes and not used for any transactions, shared a server at an off-site service provider with other websites. "Client information is not housed by the Internet service provider and has, in no way, been impacted by the accessing of the African Bank website," the bank said in a statement. African Bank IT Executive Mike King added: "Our client records and loan data were not compromised as they reside in a completely different environment" (SABCnews.com). And then, on Thursday, 24 July, the police made their arrest. According to the chief of the Western Cape's detective services, assistant commissioner Andre du Toit, a man in his 30s had been arrested at a guest house in the province after several people had been questioned. The suspect was found with five laptops, other computer equipment and documents. The following day, Johannes Jacobus Fourie, a 35-year-old Belville man, was charged with 10 counts of fraud and theft amounting to R609 714. It was revealed that the crimes had occurred between May 12 and July 18. The money was transferred into various accounts, including those of a computer company, as payment for 15 laptop computers, and allegedly into Fourier's own account to the tune of R76 025. Western Cape provincial head of detective services Andre du Toit told a media briefing on 27 July that there had been 10 complaints between May 12 and July 18 of illegal transactions from savings, personal and other Absa accounts from Durbanville, Montagu, Stellenbosch and

Paarl. The value of withdrawals ranged from R2 000 to R320 000. Fourie appeared briefly in the Bellville Magistrate's Court on Monday 28 July and remanded to August 4. It then emerged that Fourie had been employed at the Digteby Guest House, which was owned by his mother. When Absa's forensic officials examined guest house manager Katja Hiller-Staal's computer, they found a joke e-mail entitled J J Fourie on it. It appears that this e-mail was linked to the sending of an e-mail message which unleashed "spyware" onto Katja Hiller-Staal's computer, allowing bank account holders' account information to be stolen and money transferred from their accounts. The case was postponed from August 4 to August 11, then to August 12 and eventually to September 16, for further investigation. Finally, on 7 October, he was released on R10 000 bail – but the number of charges he faced were increased to 55. Prosecutor Anthony Stephen told the court he opposed bail on the grounds that Fourie had continued hacking after police caught up with him, and that he might attempt to evade trial. Stephen said that charges 37 to 55 had been committed after Fourie received a warning statement on June 26 from the police, saying that they were investigating him.

Within this context, the research question was formulated as follows:

How does the perceived risk of online and mobile delivery channels affect the likelihood of the adoption of the Digital Banking in South Africa?

In order to answer the research question, it was necessary to answer the following sub-questions:

What kind of the Digital Banking related crimes are experienced in South African banking environment?

How does the perceived credibility of online and mobile delivery channels affect the intention to adopt Digital banking?

Which technical measures are banks employing to address online/mobile banking risks and crime?

What other measures are banks employing to deal with the risk and crime related to mobile/online banking?

What are banks doing regarding the ATM bombings?

3 RESEARCH METHODOLOGY

This study on which this paper is based on employed a qualitative approach, with individual interviews, key informant interviews, and document analysis being conducted. The reason for using the qualitative approach was that respondents could constitute a rich and valuable source of information. The study went beyond the numbers and statistics.

The participants in the study were four South African banks – Investec, Nedbank, Standard Bank, and ABSA. Although the First National Bank and Wizzit did participate in the interviews, information related to these banks was obtained from their websites and public documents. According to Meulenberg-Buskens (1997:114), sampling is imperative because the researcher cannot "study everyone everywhere doing everything". In this study purposive sampling was used; participants in this study were chosen in regard to the contribution that they could make. Other than the professionals in the banking sector, other experts were also interviewed. These include a senior lecturer in security studies, a researcher attached to security institute, an Information Technology lawyer, and a financial journalist. Some interviewees requested that their identity should not be revealed since this could harm their careers. Pseudonyms have been used against extracts of their interviews.

The study used generic techniques for qualitative data collection and analysis. The study satisfied the principle of triangulation by employing multiple data-gathering methods and sources. Data-gathering methods include interviews, documents analysis, and observation.

Data gained from interviews was analysed using open coding. A frequent comparative method was applied to analyse data within and between interviews. Content analysis was also applied to analyse the content of interviews. The process involved the instantaneous coding of raw data and the construction of categories. Data was analysed with the intention to distinguish common patterns and to put together categories; these were weighed against the literature and collected documents from the banks. These categories were used to answer all the research questions. Data collected through document analysis was analysed through content analysis.

4 FINDINGS OF THE STUDY

Due to space constraints, this paper will only focus on the findings obtained through the interviews.

4.1 There are several types of Digital Banking related types in South Africa

4.1.1 Skimming

Fraudsters use skimming devices to harvest the credentials of the cheque or credit card owner. Skimming "usually happens in restaurants and hotels, the cashier or waitress would take your card away to process the payment behind the counter. Your card would then be swiped through the device and thus your User ID and password would be extracted improperly. Alternatively, both sides of your card may be photocopied."[2] The criminal downloads the gathered information from the device into a computer. The next step would be to use the downloaded information to produce a fraudulent card. "But in actual effect, the criminal can use the photocopied information successfully without necessarily manufacturing another card." These kind of crimes have made South African banking system to be more smart and superior compared to their counterparts worldwide: "the vendor machine that enables a customer to pay their bills in their tables without giving away their cards was initiated in South Africa to thwart crime."[3]

4.1.2 SIM card swop

The *SIM [Subscriber Identity Module] card swop* fraud is referred to as "*SIM card swapping or cell phone hijacking"*. In this particular crime, criminals would ask the victim's cell phone service provider to transfer the existing cell phone number onto a new SIM card by pretending to act on the victim's behalf. "*Criminals would find ways to get a copy of your authentic or falsified ID. This would convince the Vodacom, MTN, or Cell*

[2] Interview with the finance journalist

[3] Interview with researcher in a security institute

C that the request is legitimate."[4] By the time criminals swap the SIM card, they already have the victim's Online Banking User ID and password. The only thing they needed would be the OTP [One Time Password] which is transmitted via the cell phone when the account holder logs in. "*The possession of the swapped SIM card would enable the fraudsters to create new recipients within the online banking account of the victim. They will then transfer the victim's money onto the fraudulently created recipients' accounts. The fraudsters have in the past also used the OTP to increase the credit limit of the victim's account*." When all these fraudulent transactions are taking place, the bank would be sending records of transaction to the victim's cell phone; unfortunately the victim would not receive the alert SMS because his/her cell number has been swapped.

After realising that cell phones were contributing to the commission of criminal activities, the Parliament of South Africa established the 'Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002'. Amongst other things, this Act requires that the buyers of the pre-paid SIM cards should be registered by cell phones network operators so that the law enforcement agencies could identify them if and when their cell numbers are used to plan or to commit crime. A legal expert indicated that: "*the Department of Justice will announce a date in which the registration of the people who buy SIM cards commences. The delay in implementing this requirement is not justifiable, especially when you consider the fact that the Act was passed in 2002*."[5]

4.1.3 Keystroke logging

Criminals would capture the computer keystrokes of the victim. "*They would do this by either deploying a piece of hardware or some software that would harvest sensitive online banking user identity of the victim The hardware can be installed illegally into the victim's computer whilst the software can be send via an email as an attachment.*"[6] The hardware or software would be recalled and the victim's User ID and password would

[4] Interview with a manager of Interne Banking

[5] Interview with a lawyer

[6] Interview with the researcher in a security institute

be retrieved. Criminals will then use the harvested information to gain access into the victim's online bank account and defraud him/her.

4.1.4 Deposit slip scams

The criminals would deposit a cheque into the victim's account. In this instance, the victim is a merchant who is selling goods and the criminals are prospective customers who intend to purchase the goods. The copy of the deposit slip with the official bank stamp is faxed though and the victim realises the goods to criminals. "*In fact the merchant will receive the SMS from the bank alerting her that a certain amount has been deposited into her trading bank account. The criminals usually deposit the cheque on a Saturday. When the cheque is discovered on Monday to be fraudulent, the deposit to the merchant is reversed, leaving the victim out of budget.*"[7] Alternatively, the criminals would deposit a cheque which reflects more money 'by mistake' than the actual value of the goods. This would compel the merchant to give the buyer a refund.

4.1.5 Spyware

The criminal put the software in the victim's computer mysteriously. This may be done either by an email attachment or "*the victim may gullibly download the spyware from the Internet. Once the spyware is in your machine, personal sensitive information will be harvested and sent back to the criminals*"[8]. This kind of crime happens regularly in the South African online banking environment.

4.1.6 Phishing and spoofing

Criminals would conduct this crime over the phone or via the Internet or as an urgent email purporting to be from the informing victims that their account information should be updated urgently. The email would contain a hyperlink, which would direct the victim to a site that appears to be genuine, "*but in fact it has been set up by cyber-criminals to gather information provided by gullible victims*."[9] The stolen information would allow the criminals to access the online banking accounting of the victim. Another digital banking crime which is more or less similar to *pharming* is

[7] Interview with the finance journalist

[8] Interview with the manager of Internet banking

[9] Interview with security senior lecturer

spoofing "*wherein a website that resembles the official website is developed to mislead the victims into volunteering their online banking credentials*".

4.1.7 ATM bombings

The study on which this paper is based on found that the number of ATM bombings in South Africa had increased by a startling 3000 percent since 2005. This is new crime phenomenon in South Africa, and has surpassed world record. The criminals bomb the ATM into pieces and then collect the bank notes. During the interviews in participating banks, officials revealed that explosives stolen in mines were being used to destroy the ATMs so that criminals could gain access to cash once the machine has been broken into pieces. A researcher in a security institute claimed that the explosives illegally obtained from the gold mines are *"sold in a black market for up to 1100 times the normal price because the demand for these devices is very high. The situation is getting worse; you now have about 10 cases of the ATM bombings reported in a weekly basis. The ATM bombings have become a common crime."* [10] Although all banks have had their ATMs bombed, Standard Bank claims to be the most affected: "*We have more ATMs than any other bank in South Africa and thus we are mostly affected*."[11]

4.1.8 ATMs do not give the right amount of money

Some bank clients have claimed that banks robbed their money by dispensing fewer amounts than requested. A finance journalist who specialises with money matters claimed to have "*noted lots of complaints from consumers regarding this matter; this usually happens in ATMs that are found in the supermarket*." The problem is that when clients call their banks to complain and request reimbursement, the bank refuses because the bank journal will confirm that the right amount was dispensed: "*It does not mean that banks are deliberately robbing the clients but the problem is more technical and banks have to do something about this. The rollers on the dispensing system do not push the money out adequately and thus some bank notes get stuck before they are completely out of the machine.*"

[10] Interview with a researcher in a security institute

[11] Interview with Itumeleng Monale, Director of Self Service Banking in Standard Bank

During the course of the interviews for this study, banks officials refused to confirm that some of the ATMs cash dispensing problems have something to do with the criminals. Actually, they also declined to confirm that rollers in the dispensing system of some ATMs were causing problems. However, a senior lecturer in the field of security indicated that "*criminals put Card Reader (in) the ATM which would scan the clients' card information and PIN numbers. They will then proceed and manufacture their own clients' cards*". Nevertheless, the research in the security institute objected vehemently to the aforementioned claim: "*As far as I know, such type of the identity theft and ATM engineering has not yet been reported in South Africa*." The researchers of this study are therefore unable to declare conclusively if this type of crime exists or not.

4.2 The impact of the perceived credibility of Digital Banking to the adoption of the online and mobile channels is very little

South African banks try to avoid creating the perception that Digital Banking delivery channels (online and mobile) are risky "*because that in its own is a huge risk.*"[12] The image portrayed to the customers by the banks is that the aforesaid delivery channels are credible. Be that as it may, clients are made aware of the factors that enable fraud, "*this creates awareness of fraud delicacy*"[13]. Notwithstanding, some customers tend to become concerned about security issues, especially when it comes to the online banking delivery channels. However, as time goes on users become comfortable with the delivery channel; that is why when the online banking was launched, *"people said they never bank on the Internet – the Internet is one of the most dangerous places"*. As the delivery channels mature, users become comfortable; so the impact of security concern has very little impact in the adoption of Digital Banking delivery channels. Officials in the banking industry were at pains to explain that customers in South Africa, especially the 'middle and upper classes' would rather conduct banking transactions using the Internet and mobile devices rather than frequenting the ATM. Certain security expert emphasised this point: "*You'd have heard about a gang that is observing customers when they withdraw money either from the teller or ATM; if they appear to have withdrawn a huge amount, they are then followed and*

[12] Interview with Domini Takacs, Senior Channel Manager: Cellphone & Electronic Channels in Nedbank

[13] Interview with Lee Albertyn, Head of Virtual Channels in Nedbank

robbed outside the shopping mall. This kind of crime drives the rich, I mean the personal bankers to the online and mobile deliver channels." According to Christo Very, Managing Executive of Digital Channels in Absa, customers who are not adopting the Digital Banking channels are mostly affected by accessibility and affordability of computers and the Internet rather than the perceived lack of credibility of the Digital Banking.

4.2 Banks employ advanced technical measures to fight Digital Banking crimes

South African banks have dedicated teams of information security specialists who "combat' cyber crimes. Seeing that customers are concerned with Digital Banking crime, banks are reacting to crime aggressively and with a lot of sophistication; to avert losses, especially of assests and reputation[14]. Amongst other measures, phishing and spoofing websites are removed and suspicious emails are blocked before they reach the customer. This statement is supported by Christo Vrey[15]: "*We ensure that we have got monitoring systems, behaviour pattern analysis, and early warning systems, for example, if spoofing site is picked up worldwide on the Internet or a phishing email goes out, we typically shut the site down within 45 minutes to two hours. It doesn't matter where it sits in the world.*" Banks are also 24 hours available to assist their customers in case they suspect they are being defrauded online. They can phone the contact centre "*and there is also a button in the Internet banking that says "do you want to report a fraud incident", press the button – they will close your account immediately.*" Banks are also making positive progress when it comes to the thwarting of the SIM swop crime. They are working with the mobile telecommunications network operators to eliminate this crime: "*As far as mobile banking is concerned, Standard Bank has spoken with Vodacom regarding the SIM swop fraud. Vodacom has implemented a process whereby a notification SMS is sent to both the old and new SIM card regarding the SIM swaps. They also marry the serial numbers of SIM card with the cell phone's serial number.*

[14] Interview with Kobus Burger, Head of Private Bank Account in Investec

[15] Managing Executive of Absa Digital Channels

This has helped a lot in reducing and discouraging the unlawful SIM swops."[16]

Some banking officials claimed that there are instances wherein they actually literally stop the money from leaving the system fraudulently: "*we actually recovered a large percentage of money. It actually gets stopped, so there are whole set of aspects that the bank does arousing facilitating secure online banking.*"[17] Banks ensure that online banking transactions are taking place in a secure encrypted environment. It is impossible for the criminals to intercept these kinds of transactions because of encryption. The signature by the end side of the encryption is done by certificate imbedded in systems in the bank, in browser, so whenever customers see the lock, they know they are in the genuine banking website. Other than the lock, users would also look at the URL.

Some of the methods employed by the banks to combat e-crime are very controversial. These include the fact that some of the banks hire their own hackers and bomb their own ATMs. Working very closely with the law enforcement agencies and the South African Banking Risk Information Centre, banks have managed to bring down the level of the ATMs bombings. The South African Police Service's National Intervention Unit has been in the forefront of curbing the ATMs bombings. This has been achieved by arresting and killing the criminals responsible for this crime. Some of the intended ATMs attacks were foiled by the banks working together with the police. A Director of the Standard bank Self-Service Banking claimed that: "*Due to the fact that our ATMs are mostly hit, we decide to enhance the security around the ATMs. New ATMs are less penetrable and are environmentally friendly in case they are successfully bombed. The bank has mechanisms to detect when ATM machines are being tempered with. We have worked very closely with the police and about 400 perpetrators have already been arrested*."

4.3 Banks spend billions of rands to train users in security

Customer training helps to improve the perceptions regarding the credibility of the Digital Banking delivery channels. Banks also avoid

[16] Dheena Govender, Head of Internet Banking, Self-Service in Standard Bank
[17] Interview with Abdul Noutcha, Webmaster of web channel for Self –Service in Standard Bank

litigation, poor adoption of cell phone and mobile delivery channels by ensuring that users are adequately trained. It is in this premise that banks have refused to pay customers money defrauded through Digital Banking crimes. Education is a priority in all the banks and thus "*there is frequent employee and customer education regarding security*". According to Christo Vrey[18]: "*If we go back to 2003, where we had the incident where a client, when key logging was put onto his PC in the Eastern Cape and he was defrauded of money through cell phone engineering. The biggest criticism we faced shortly after the announcement was from the client's point of view, "how have you kept us informed about what risks are in the Internet banking?" If I look at where we were then and where we are now, that picture has changed fundamentally; we spent many billions of rands annually as the industry around the awareness campaigns.*" Each of the four big banks posts vast security related materials on their websites. Newsletters are also sent to the clients on a quarterly basis to provide security related tips to the clients. Banks are proactive in warning the clients.

The South African banks are proactive when it comes to crime and they have got early warning mechanisms that enable to see what is happening globally regarding the security of their customers' accounts. The aforesaid mechanisms put the South African banks in a position to be informed of security threats before they actual manifest. On the other hand, if the crime happens, affected clients are informed speedily. Information security intelligence provided to the customers has increased drastically since the first famous Digital Banking crime in South Africa 2003.

4.4 Banks expect clients to be responsible for their accounts' security

When Digital Banking related crimes were reported for the first time in South Africa in 2003, banks would reimburse the clients. However, banks currently refuse to reimburse the clients because they are doing a lot to educate and support the clients. This includes providing clients with the "freebies" to enhance their security. Christo Very becomes very emphatic to stress the point: "*There are the client's responsibilities as he conducts*

[18] Managing Executive of Absa Digital Channels

his life on the internet that we cannot control, we can inform him. We will give him free of charge, the best available anti-virus application off the shelve costing between R700 and R800." It is the responsibility of the client to ensure that the antivirus software is deployed in his/her computer. This would assist in making the computer safe. 'For free', banks give an SMS when a user logs into the Internet banking: "*If you get an SMS and you are not doing the Internet banking, then there's a problem.*"[19] There is a telephone number contained in the SMS that banks dispatch to the client. The client can call this number the moment they become suspicious regarding security in their Digital Banking accounts. Users should ensure that they do not conduct transaction in the unsafe computing environment like the Internet cafes.

If the client decides to ignore SMSs from the bank regarding transactions that are taking place in his account, then the bank cannot be expected to be liable: "*So if the client is going to be negligent in his behaviour, he is going to have problems. So, if you can see, if he gets an SMS at two o'clock in the morning and he is not busy working on his PC and he choose to go to sleep without contacting the bank, he will lose money and the bank cannot be liable.*" [20] The South African banks are becoming more sophisticated in terms of ensuring that clients are more secured in the Digital Banking environment: "*You'll notice that at Absa, we use a bit of a different approach than most banks do in South Africa. We've got a two stage approach to log in, so what it does is, it gives us an opportunity to go back to the client before he is fully into online banking and confirm with the client that he's actually at the right place. We've created a phrase called Sure Phrase and in essence we bring to you a message that you've personally personalized in internet banking that tells you before you go through with the next page. You can check if that message is there. Now, if it's not there, that means you're on a fake site that looks like the Absa site but is actually not. There's a lot of sophistication there that we bring from Absa point of view to our process, that's been very successful for us and something that we continue to educate our clients on*"[21]. Absa is also the only bank which has a Virtual

[19] Interview with Lee Albertyn, Head of Virtual Channels in Nedbank
[20] Interview with Domini Takacs, Senior Channel Manager: Cellphone & Electronic Channels in Nedbank
[21] Interview with Christo Very, Managing Executive of Absa Digital Channels.

Keypad for the Internet banking. The Virtual Keypad makes it impossible to steal the client banking credentials through keystrokes logging.

5 CONCLUSION

The findings of this study appear to reveal that the adoption of the Digital banking is not adversely affected by online and mobile delivery channels security concerns. The researchers of this study found that the crime level in South Africa is actually pushing people into Digital Banking products. One would be very sceptical to go around with a lot of cash in South African streets. Even if you have a car, it can be stolen or hijacked with your money. When the authors of this paper were busy composing the report on which this paper is based on, they read an article in *The Star* (13 April 2009) which reported on the crimes committed Bank Queue Gang. It is the authors' contention that such crimes will drive more people to adopt the Digital Banking deliver channels. According to the article: "By definition, the crime occurs when a client leaves a bank, is followed and robbed. The victims are often tradesmen, who draw large amounts of cash on a Thursday to pay their casual labourers the following day. The linchpin of the gang is the "spotter". Spotters blend in, wait in bank queues and look for a target. Sometimes, they don't even need to see the money; they hear it. They will listen for the noise of the cash machine counting out money. To make themselves appear legitimate, spotters will deposit small amounts of cash or ask a teller for change. Using a cellphone, the spotter will then quickly pass on information. They will describe what their target is wearing and sometimes even inform the "shooters" outside in which pocket the money is being held. Outside, the shooters will pick up the target and begin following on foot or by car. The actual hit is quick and sometimes the gang is violent. Bank customers are not just followed. Sometimes the robbers strike as they head to the bank to deposit money. The challenge here is the fact that this type of crime is traditionally underreported and therefore there is no sufficient data to benchmark against. Bank staff also advise clients of alternative banking products, such as electronic transfers, and warn them of the dangers of carrying large sums of money when assisting them with transactions involving large cash withdrawals." Another driver to the Internet and mobile banking is the ATM bombings. ATMs users are concerned that they may become victims of the ATMs bombings.

The irony of this crime is that South African banking system to be the best in the world in terms of technology sophistication. Banking in South Africa includes wireless ATMs in remote areas. Wireless signals are used to link a point-of-sale credit card reader into banking system, allowing small vendors to accept credit cards. The attendant brings a mobile payment devise that allows customers in a restaurant to pay bills of their meals on their tables. The waitress does not have to go behind the counter with the customer with customers' debit or credit cards; this prevents crimes such as identity fraud and *skimming*. The South African banks are far ahead of the American and European banks regarding introduction of mobile and electronic banking products.

6 REFERENCES

Goldstuck, A. 2006. Online Banking in South Africa. World Wide Worx: Johannesburg.

Goldstuck, A. & Dagada, R. 2009. The 2008 World Wide Worx and Wits Business School Digital Banking Research Report. World Wide Worx: Johannesburg.

Meulenberg-Buskens, I. 1997. Turtles all the way down? -on a quest for quality in qualitative research. South African Journal of Psychology, 27(2): 111-116.

Smillie, S. 2009. Beware of deadly 'bank queue gang'. *The Star*, 13 April 2009. Independent Online: Johannesurg.