ABSTRACT

This paper addresses aspects of security in the following digital banking delivery channels: Internet, cellphone and Automated Teller Machine (ATM). South African banks use these delivery channels to reduce operational costs and enable customers to conduct banking transactions conveniently. This study found that the adoption of digital banking services in South Africa is growing tremendously. This has attracted criminal elements employing tactics such as skimming, SIM (Subscriber Identity Module) card swapping, ‘phishing’ and ‘spoofing’, ATM bombings, and SMS (Short Message Service) interception. Because customers are extremely concerned about digital banking crime, South African banks are dealing with the crime swiftly and with a great deal of sophistication. The study has found that the adoption of digital banking services is not negatively affected by security concerns. In other words, the credibility of digital banking remains intact despite security issues.

KEYWORDS

Digital banking delivery channels, security concerns, measures to fight crime, credibility of digital banking services

1. INTRODUCTION

The cost-to-income ratio is debatably one of the most significant ratios in any bank’s yearly reports. It indicates how much of every South African rand earned contributes to the bank’s running costs and, therefore, how proficient the bank is in creating value for its shareholders. In their pursuit of an improved ratio, South African banks focus on moderating customer dependence on branches by encouraging the use of cheaper self-service delivery channels such as the Internet, cellphones and ATMs [1]. The banking industry views the digital banking service as a means of reducing operating costs and retaining customers [2].

The term ‘digital banking’ in this study refers to the use by customers of the Internet, cellphones and ATMs as banking delivery channels. ‘Online banking’ refers specifically to the use of the Internet for banking transactions, while ‘cellphone banking’ is defined as the employment of mobile phone devices to conduct banking activities.

The Internet was launched in South Africa in or around 1996 and was followed by cellphone banking services in 2000 [3]. The subscriber base for digital banking in South Africa reached 5 719 280 by March 2009. Of this figure, 3 642 340 represented Internet banking subscribers, while cellphone banking customers numbered 2 076 940 [4]. This is a far-reaching development when one reflects on the World Wide Worx’s 2006 Online banking in South Africa report. According to this 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”. The researcher found that the number of digital banking accounts grew rapidly from 2005. The growth in digital banking has continued despite the security concerns of both banking executives and customers.
Mobile network operators in South Africa have contributed immensely to the introduction and adoption of cellphone banking in South Africa [5]. The operators, Vodacom, MTN and Cell C, have a customer base of just over 40-million subscriptions. However, it is the researcher’s view that the uptake in cellphone banking, totalling 2.7-million users, is not that impressive when one considers the fact that cellphone subscriptions total just over 40-million. There is a significant mismatch between the number of cellphone subscriptions and the number of customers adopting cellphone banking. Be that as it may, it is my contention that the adoption of cellphone banking will surpass that of Internet banking by mid-2011. This is attributed to the fact that the pace of cellphone registrations is growing faster than those of the Internet [6]. In effect, Internet banking is reaching saturation point. The number of Internet users in South Africa is just over 4.6-million, while the number of customers using Internet banking is around 3.6-million. However, for many years to come, Internet banking will remain more profitable for banks because of the number and value of transactions. The researcher is not arguing that Internet banking will not grow. It will, but more conservatively than cellphone banking.

The growth in the adoption of digital banking services in South Africa has attracted the attention of criminals who wish to benefit from a booming industry [7]. This study will show that the level of sophistication of digital banking crime in South Africa is extraordinary. This paper will also reveal that the majority of digital banking-related crimes affect Internet and ATM banking. This study has found that there has never been any cellphone banking crime in South Africa.

The next sections of this paper deal with the framework of the study, research methodology and findings.

2. FRAMEWORK OF THE STUDY

The framework of this study is constituted by the literature review, which deals with Internet banking, cellphone banking, and the onset of digital banking crime in South Africa.

The next subsection addresses Internet banking in South Africa.

2.1 Internet Banking in South Africa

The Internet, as a delivery channel in the South African banking industry, has deeply altered the traditional manner in which banking transactions were conducted [8]. Millions of people are able to conduct banking transactions through the Internet instead of going physically to a branch of the bank as has been the norm. The Internet plays a crucial role in digital banking by adding new value to self-service banking [9]. Internet banking has brought much convenience to South African subscribers [10]. They are now able to pay accounts, book flights, make purchases and transfer cash without leaving the comfort of their homes or offices. In addition, Internet banking customers do not necessarily have to access a networked PC or laptop as they are able to complete banking transactions through accessing the Internet via their cellphones.

The steady growth of access to the Internet in South Africa has contributed to the uptake in Internet banking services. The number of Internet users had grown by 12.5% to more than 4.6-million by the end of 2008, compared to 4.07-million in 2007 [11]. Goldstuck further predicts that access to the Internet in South Africa in the next five years will continue to escalate as it has in the past 15 years. In 2008 Internet penetration grew by more than 8% for the first time. Based on this premise, World Wide Worx has predicted that Internet usage will grow rapidly, reaching the 9-million mark by 2014. It is our contention that this will auger well for Internet banking.
It is important to state that, inasmuch as some South Africans are enjoying its benefits, Internet banking has raised some serious security challenges [12]. Conversely, Internet banking related crimes are regularly reported by the media in South Africa[13].

The next subsection deals with the cellphone banking in South Africa.

2.2 Cellphone Banking in South Africa

Cellphone banking was first introduced in South Africa in August 2002 when a total of 31 426 customers registered for the service [14]. By then, cellphone banking offered very limited transactions. In fact, there was only one transaction – balance checking. The first bank to launch this service was Absa. Thereafter FNB, Standard Bank and Nedbank introduced cellphone banking. Absa and FNB remain dominant in this market, while Nedbank is making huge strides despite being the last of the four big banks to offer cellphone banking services. Although Standard Bank showed very little appetite for and aggression in this market, this bank will go down in the history of world cellphone banking for being the first (in 2003) to move beyond balance checking, by enabling its Vodacom pre-paid customers to recharge cellphone airtime [15]. Before then airtime had been purchased through SMSs. It is interesting to note that today cellphone banking provides an assortment of transactions, making South Africa the market leader worldwide [16].

There are several South African banks that provide cellphone banking services; these include the four dominating banks – Standard Bank, Nedbank, Absa, and FNB [17]. These banks use cellphone banking as one of their digital delivery channels, whereas for Wizzit and MTN banking cellphone banking is a standalone offering [18]. Cellphone banking in South Africa has three formats: Wireless Application Protocol (WAP), Wireless Internet Gateway (WIG), and Unstructured Supplementary Service Data (USSD).

2.3 Wireless Application Protocol

All of the above-mentioned banks have employed WAP technology for their cellphone banking. WAP technology allows the user to access the Internet banking using a cellphone. WAP is user friendly because it offers users the same transaction interface they get from Internet banking, via the cellphone [19]. Another advantage of WAP technology is that it gives the cellphone a capacity similar to that of Internet banking. The disadvantage of WAP technology is that it excludes users whose cellphone handsets are not sophisticated. In addition, the service requires experience of the Internet [20]. The majority of cellphone banking customers in South Africa have not used the Internet at all.

The next section addresses another format of cellphone banking in South Africa called Wireless Internet Gateway.

2.4 Wireless Internet Gateway

WIG technology enables secure cellphone banking [21]. Security is enhanced by the encryption of the transactions. Unlike WAP, which has a real Internet capability, WIG downloads the bank menu onto the user’s SIM card to enable transactions. Transactions are conducted by sending requests via SMSs. WIG is actually the oldest cellphone banking technology. This technology is more accessible by users at lower economic levels. This could be attributed to the fact that it does not require expensive and sophisticated cellphone handsets.

The next subsection gives a brief overview of Unstructured Supplementary Service Data.
2.5 Unstructured Supplementary Service Data

Three South African banks, Absa, Nedbank, and FNB, have adopted a cellphone banking technology called USSD [22]. In the last few years this technology has been used in South Africa to enable mobile commerce with the emphasis on the sales of content service such as ringtones, cellphone wallpapers and music. Interestingly, FNB and Absa have extended the USSD platform to the cellphone banking sector. USSD technology is embedded in cellphone technology regardless of the handset make and the year of manufacture. Therefore, USSD works for all cellphones while WAP does not function in older handsets [23]. The USSD platform gives users prompt access to their balances and account statements and the ability to buy prepaid airtime. This technology allows very low daily and monthly limits for prepaid airtime purchases. This could be ascribed to the fact that USSD has a lower security rating than WIG or WAP.

Cellphone ownership is growing tremendously in South Africa. Stafford Masie, former Country Manager for Google South Africa, has said [24]:

Google statistics on cellphone use in South Africa showed that one in six Google searches in the country happened on a [cell] phone. This is the highest ratio of Google search on a cell [phone] in the world. Seventy-eight percent of people who own mobile phone in South Africa don’t have PCs. More than 85% of that number will never own a PC in their lifetime. The closest device to a computer they then come into contact with is the cellphone. (Bamjee-Mayet, 2009)

South African banks are not blind to these developments and are gearing up to increase the uptake in cellphone banking. The increase in uptake will assist in reducing operational costs and improve cost-to-income ratios. Over and above this, cellphone banking will provide the banks with more business and [25].

Cellphone ownership in South Africa was estimated to be around 46.6-million by 2009. This implies that cellphone ownership in South Africa is well over 100% of the population. The growth of cellphone ownership did not boost the uptake in cellphone banking in South Africa. It has already been stated that by March 2009, 2 076 940 customers had adopted cellphone banking in South Africa. There is a great discrepancy between cellphone ownership and cellphone banking services uptake. It was on this premise that the researcher decided to investigate how digital banking crime, risk and credibility affect the adoption of cellphone banking in South Africa.

2.6 The first digital banking crime in South Africa

The content in this section has already appeared in the World Wide Worx’s Online Banking in South Africa report of 2006. However, I deem it necessary to repeat the content because it provides very valuable information regarding the history of security, risk and credibility of the digital banking services in South Africa. In effect, it provides essential background to the new information contained in this paper.

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 Absa bank account. 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 deposited. When she called up her balance, the whole amount had disappeared. Within weeks, these two women would discover that they had played a role in the tensest 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 contacted Absa, which 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. 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 confirmed that week that it was investigating nine cases involving theft 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 the accounts. Police confirmed that total losses of R230 000 had been reported to them. On Friday 18 July, attorney Harry de Villiers found R300 000 missing from one of his trust accounts when he checked his statements. 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 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 alerted him only to R10 000 that had been mysteriously transferred into one of his accounts earlier in the week. Later, when he checked his accounts more closely, he discovered that amounts of R227 000 and R93 000 had been transferred to another account. Upon further inquiry, it emerged that the fraudster 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 that the fraudster had sent unsuspecting clients an e-mail which, when 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."

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

2.7 How does the perceived risk of Internet, cellphone and ATM banking affect the likelihood of the adoption of digital banking services in South Africa?

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

- What are the digital banking related crimes that are experienced in South African banking environment?
- Which measures are banks employing to address digital banking related crimes?

In order to answer the above questions, I undertook research fieldwork based on research methodology elucidated in the next section.

3. RESEARCH METHODOLOGY

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

The participants in the study were four South African banks – Investec, Nedbank, Standard Bank and ABSA. Although First National Bank and Wizzit did not participate directly in the interviews, information related to these banks was
obtained from their websites and public documents. According to Meulenberg-Buskens [26], 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 with regard to the contribution that they could make. Other than banking sector professionals, other experts were interviewed. These included a senior lecturer in security studies, a researcher attached to a security institute, an Information Technology lawyer, and a financial journalist. Some interviewees requested that their identity should not be revealed, as this could harm their careers. Generic job titles have been used for extracts from their interviews of those interviewees who did not want their names to be published.

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, document 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 of distinguishing common patterns and creating 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.

The next section deals with the findings of the study.

4. FINDINGS OF THE STUDY

The findings contained in this section deal with the nature of digital banking crimes, measures introduced to deal with crime, and preventive training. Details of the findings are reflected in the subsections below.

Findings regarding the nature of digital banking crimes

This study identified the following types of digital banking crimes: skimming, SIM card swapping, ‘phishing’ and ‘spoofing’, ATM bombings, and SMS interception.

4.1 Skimming as a digital banking related crime

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.” (Financial journalist, personal communication)

The criminal downloads the gathered information from the device into a computer. The next step is 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 kinds of crimes have made the South African banking system smarter than and superior to their counterparts worldwide: “The vendor machine that enables a customer to pay their bills at their tables without giving away their cards was initiated in South Africa to thwart crime.” (Researcher attached to a security institute, personal communication)

The South African Banking Risk Information Centre (Sabric) has reported that statistics showed that counterfeit cards which are the product of
skimming, accounted for 60% of the banking industry card fraud in the first half of 2009 (https://www.sabric.co.za). Between January and June 2009, Gauteng, the Western Cape and Kwazulu-Natal recorded the highest number of incidents. According to Sabric, fraudsters illegally produce a counterfeit card from the information skimmed from the magnetic strip of the legitimate card. Shockingly, 129 hand-held skimming devices were found by law enforcement agencies between June and September 2009, almost the same number of devices recovered for the whole of 2008.

Some bank clients have claimed that banks have stolen their money by dispensing lesser amounts than requested. A financial journalist claimed to have “noted lots of complaints from consumers regarding this matter; this usually happens in ATMs that are found in the supermarket” (Personal communication). This journalist claims that, when clients call their banks to request reimbursement, the bank refuses because the bank journal confirms that the right amount has been 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 (Personal communication).

The fact is that perpetrators of bank fraud are now targeting ATMs.

During the interviews for this study, bank officials refused to confirm that some ATM cash-dispensing problems are related to criminal activity. They also declined to confirm that rollers in the dispensing systems of some ATMs were causing problems. However, senior lecturer in security studies indicated that “criminals put a 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”. However, the researcher attached to a security institute objected vehemently to this claim: “As far as I know, such type of identity theft and ATM engineering has not yet been reported in South Africa.” Nevertheless, as the researcher of the study on which this paper is based, I can conclusively confirm that criminals in South Africa are attaching skimming devices to the slots of ATMs to harvest information and clone bank cards. Some digital banking criminals are qualified engineers and there is thus a high level of sophistication.

4.2 SIM card swapping as a digital banking related crime

SIM card swap fraud is referred to as “SIM card swapping or cellphone number hijacking”. In this particular crime, criminals request the victim’s cellphone service provider to transfer the existing cellphone 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 Vodacom, MTN, or Cell C that the request is legitimate.” (Manager of Internet Banking) By the time criminals swap the SIM card, they already have the victim’s online banking user ID and password. The only thing they would still need is the One Time Password (OTP) which is transmitted via the cellphone 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.”

While these fraudulent transactions are taking place, the bank sends records of transaction to the victim’s cellphone; unfortunately the victim does
not receive the SMS alert because his/her cell number has been swapped.

Recognising that cellphones were being used to commit crime, the South African Parliament passed the ‘Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002’. Among other things, the Act requires that buyers of pre-paid SIM cards should be registered by cellphone network operators so that law enforcement agencies can identify them if and when their cell numbers are used to plan or to commit crime. A legal expert indicated:

The Department of Justice announced 1 July 2009 as 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. (Information Technology lawyer).

The registration of cellphone SIM cards as required by law was implemented seven years after the promulgation of the Act.

4.3 ‘Phishing’ and ‘spoofing’ as digital banking related crimes

Criminals conduct these crimes via the phone, Internet or an urgent email purporting to be from the bank. Victims are informed that their account information should be updated urgently. The email contains a hyperlink, which directs 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”. (Senior lecturer in security studies, personal communication) The stolen information allows the criminal access to the online banking account of the victim. A digital banking crime similar to ‘pharming’ is ‘spoofing’ “wherein a website that resembles the official website is developed to mislead the victims into volunteering their online banking credentials”.

4.4 ATM bombings as digital banking related crimes

The study on which this paper is based found that the number of ATM bombings in South Africa has increased by a startling 3 000 percent since 2005. This crime phenomenon in South Africa has surpassed the world record. Criminals destroy the ATM with explosives and then collect the bank notes. During interviews with participating banks, officials revealed that explosives stolen from mines were used to destroy ATMs. A researcher attached to a security institute claimed that the explosives illegally obtained from gold mines are: sold in a black market for up to 1 100 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.

Although all banks have suffered ATM bombings, 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.” (Itumeleng Monale, Director of Self Service Banking in Standard Bank). This underscores the fact that ATM banking crime is a serious risk to the financial sector.

4.5 SMS interception as digital banking crime

On 12 July 2009, The Citizen [27] reported on what is so far the biggest Internet banking scam in South African history. The amount stolen through this scam is estimated to be R7-million. According to The Citizen, the syndicate was aided by 39-year-old Vodacom engineer, Mbokodana Christopher Khoza, who holds a BSc degree in Engineering. The syndicate siphoned money from Internet banking clients of Nedbank, Absa,
Capitec, FNB, Standard Bank and Ithala Bank. Several members of the syndicate were arrested and Vodacom has laid criminal charges against Khoza. The mobile operator is also working with Sabric and the South African Police Services (SAPS) to deal with this scam. In an internal memorandum, Vodacom informed its employees of the first scam of this kind in the world and requested staff to convey the facts to their families, friends and customers. The statement reads as follows:

The online banking customers had to somehow compromise their PIN and password, typically through a phishing and/or spoofing attack where a false website is used. This PIN and Password gave scammer access to the online banking account, but to create a new beneficiary and transfer money a One Time Password (OTP) is needed. This poses two hurdles: gaining access to the cellphone number of the account holder to which the OTP is sent via SMS and then intercepting the OTP SMS without the owner knowing about it. Obtaining the account holder’s cellphone number was typically achieved either by social engineering or by the same phishing scam which gave the fraudsters access to the account holder’s banking details. Intercepting the OTP SMS without the owner knowing about it is where the rogue Vodacom employee came in. The Vodacom employee created a temporary dual SIM, active online for a very short period of time, to intercept the OTP SMS. This OTP was forwarded to the syndicate which had by now logged into the banking account and was awaiting the OTP to create a new beneficiary and transfer money to this new beneficiary. The short time frame in which the false dual-SMS is active means that the legitimate owner of the SMS was typically unaware of the downtime and therefore would not suspect anything untoward. After the money has been transferred to the fraudulent account it is withdrawn as quickly as possible. To ensure a speedy transfer of money the syndicate typically used a fraudulent account from the same bank as the victim who was scammed.

It is disturbing to note that the Financial Intelligence Centre (FIC), an offshoot of the Financial Intelligence Centre Act (FICA) of 2001, failed to discover this SMS interception scam and many other incidents where money was siphoned through digital banking delivery channels. The FICA and FIC were introduced recently in South Africa to assist in combating money laundering.

The next section focuses on the impact of credibility on the adoption of digital banking services in South Africa.

4.6 Findings regarding measures that are employed by the banks to manage crime

This study found that the South African banking industry uses both technical measures and education to eradicate digital banking related crimes. More details regarding these measures are contained in the subsections below.

4.7 Technical measures used by the banking industry to fight digital banking related crimes

South African banks have dedicated teams of information security specialists to combat cyber crimes. Because their customers are concerned about digital banking crime, banks are reacting to crime aggressively and with great sophistication in order to avert losses, especially of assets and reputation (Kobus Burger, Head of Private Bank Accounts, Investec). Amongst other measures, ‘phishing’ and ‘spoofing’ websites are removed and suspicious emails are blocked before they reach the customer. This is supported by Christo Vrey:

We ensure that we have got monitoring systems, behaviour pattern analysis, and
early warning systems, for example; if a 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. (Christo Vrey, Managing Executive, Absa Digital Channels).

Banks have established 24-hour contact centres to assist customers who suspect they are being defrauded online. “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 SIM swap crime. They work with mobile telecommunications network operators.

As far as mobile banking is concerned, Standard Bank has spoken with Vodacom regarding the SIM swap 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 cellphone’s serial number. This has helped a lot in reducing and discouraging the unlawful SIM swaps.” (Dheena Govender, Head of Internet Banking, Self-Service, Standard Bank)

Some banking officials claimed that there are instances where they are able to prevent 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 around facilitating secure online banking.” (Abdul Noutcha, Webmaster of Web Channel for Self-service, Standard Bank)

Banks ensure that online banking transactions take place in a secure and encrypted environment. Encryption prevents criminals intercepting these kinds of transactions. The signature at the end of the encryption is secured by certificates embedded in the bank systems and browser. Whenever customers see the icon of a lock, they know they are in the genuine banking website. Other than the lock, users can also inspect the URL.

Some of the methods employed by the banks to combat e-crime are highly controversial. Some banks hire their own hackers and bomb their own ATMs. Working very closely with law enforcement agencies and Sabric, banks have managed to reduce the number of ATM bombings. SAPS’s National Intervention Unit has been in the forefront of curbing ATM bombings. This has been achieved through aggressive policing and successful arrests. Some planned ATM attacks have been foiled by close cooperation between the banks and the police. A Director of Standard Bank’s Self-Service Banking claimed:

Due to the fact that our ATMs are mostly hit, we decided 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 tampered with. We have worked very closely with the police and about 400 perpetrators have already been arrested.

Absa was the first bank in the world to craft another interesting method to curb digital banking crime, particularly ATM skimming and bombings. This method involves squirting pepper-spray into the face of the criminal while he is tampering with the machine. The technology also uses cameras to identify these criminals. At the time of finalising this report, Absa’s use of this method was still in the pilot stage. If the pilot study yields positive results, Absa will roll out this technology nationwide. Other banks are likely to follow suit. Certainly, South African banks appear to be working tirelessly to stay one step ahead of highly sophisticated criminals.
4.8 User training as a preventive measure

Customer training helps to improve positive perceptions regarding the credibility of digital banking delivery channels. Banks endeavour to avoid litigation, and to combat poor adoption of cellphone and mobile delivery channels by ensuring that users are adequately trained. Based on this premise, banks have refused to reimburse customers 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:

If we go back to 2003, we had the incident where [an Eastern Cape] client, when key logging was put onto his PC...was defrauded of money through cellphone 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 Internet banking?’ If I look at where we were then and where we are now, that picture has changed fundamentally; we spend many billions of rands annually, as the industry, around the awareness campaigns.”

Each of the four big banks posts extensive security-related materials on their websites. Quarterly newsletters are also sent to clients providing security-related tips. Banks appear to be proactive in warning the clients.

Not only are South African banks proactive when it comes to crime, they also have early warning mechanisms enabling them to see what is happening globally regarding the security of their customers’ accounts. These mechanisms put South African banks in a position where they are informed of potential security threats before they actually occur. On the other hand, if the crime is successful, affected clients are informed speedily.

Intelligence regarding information security provided to customers has increased considerably since the first famous digital banking crime in South Africa 2003.

When digital banking related crimes were reported for the first time in South Africa in 2003, banks would reimburse their clients. However, banks currently refuse to do this because they believe they are doing more than enough to educate and support their clients. This includes providing clients with “freebie” software to enhance security. Christo Vrey is very emphatic:

There are a client’s responsibilities as he conducts 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 shelf costing between R700 and R800.”

It is the responsibility of the client to ensure that the antivirus software is installed on his/her computer. Banks also send an SMS when a user logs onto Internet banking: “If you get an SMS and you are not doing Internet banking, then there’s a problem.” (Lee Albertyn, Head of Virtual Channels, Nedbank) The SMS includes a telephone number that the client can call as soon as they become suspicious regarding security breaches in their digital banking accounts. Users are warned not to conduct transactions in unsafe computing environments like Internet cafes.

5. CONCLUSION

The findings of the study suggest that the adoption of digital banking is not adversely affected by security concerns regarding online and mobile delivery channels. The researcher found that crime is encouraging South African customers to move away from cash transactions to digital banking services. When the author of this paper was finalising this report, an article in The Star (13 April 2009) reported on crimes committed by the ‘Bank Queue Gang’. It is the author’s contention
that such crimes will drive more people to adopt digital banking delivery channels. According to the article [28]:

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 not 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. (Smillie, 2009)

Another factor encouraging the shift to Internet and mobile banking is the threat of ATM bombings. ATM users are concerned about their personal safety.

The irony surrounding digital banking crime is that the South African banking system is regarded as the best in the world in terms of technological sophistication. There are a number of innovations in use: wireless ATMs in remote areas; wireless signals linking a point-of-sale credit card reader to the banking system, allowing smaller vendors to accept credit cards; mobile payment devices allowing restaurant customers to pay at their table, with their bank cards within sight. It is clear that South African banks are far ahead of American and European banks regarding the introduction of mobile and electronic banking products [29].

REFERENCES


