Management Information System: Few Tips Befitting Small Businesses to Avert ID Theft Critical of Illicit Technology

NAFTA MOKATE LEHOBYE
Tshwane University of Technology
State Artillery Road,
Pretoria-West Republic of South Africa

Dr. K. SREENIVASA VIJAYA SIMHA
Researcher
Andhra Pradesh,
South India

Abstract- **Carrying large sums of money everywhere has long been seen cumbersome and provocative practice to criminals. Later this practice was viewed unprofessional within business and corporate practice and was thus replaced by cheques and lately by bank cards loosely referred to as plastic money. Despite all, one-man small businesses should also use a cheque to withdraw money from their current bank accounts like macro businesses; it still makes a lot of real sense when they use bank cards just for a start for their cash withdrawals. Given these, all entrepreneurial efforts taken when establishing these businesses to avoid legal and financial risks, there is still much out there to look out for to protect their cash when effecting deposits and withdrawals using black stripped bank cards. These entrepreneurial management strategies are tailor-made to help small firms which have just been established as they have not as yet fully established themselves evade ID theft. In order to achieve to avert this kind of crime, this paper will then provide few tips as management strategies befitting small firms to rather circumvent the said crime. This paper also takes cognisance of what the South African (SA) law actually says to protect small firms from this particular financial risk brought about by this crime.**

Keywords: Entrepreneurialism; ID Theft; Management Information Systems; Legal Positioning

I. INTRODUCTION

We all know that carrying large sums of money everywhere has never been a good idea at all especially when considering the crime levels bedevilling every one including even small businesses. Carrying a hundred thousand rand of loose hard cash in one's possession for example may prove very fatal and has thus long been seen cumbersome and an extremely provocative practice to criminals. Later, this practice was viewed unprofessional within the business context and corporate cycles and was thus replaced by cheques as a turnaround strategy (Akrani, 2012) and now lately by bank cards (Carpenter, 2012) loosely referred to as plastic money (Larry, 2010). Despite all, one-man businesses should also use a cheque to withdraw money from their current bank accounts the same as with macro businesses; it still makes a lot of real sense when they use black striped bank cards just for a start for their cash withdrawals. But where does this lead small business to? Given these, all efforts taken when establishing these businesses to avoid legal and financial risks, there is still much out there to look out for to protect their cash when effecting deposits and withdrawals using black stripped bank cards. These entrepreneurial management strategies are tailor-made to help small businesses avert identity (ID) crime. In order to achieve to avert this kind of crime, this paper will then demystify its manifestation by providing a few tips as management information systems befitting small businesses to rather circumvent the said crime. This paper also takes cognisance of what the South African law actually says to protect small businesses from this particular crime.

II. RESEARCH METHODOLOGY

This qualitative research study essentially demystifies the manifestation of ID theft by defining the ID theft itself and then describing a few tips befitting small businesses. It will define the management information systems (MIS) within the context of small businesses and show through snap interviews how disturbingly fatal this crime can prove to be to small businesses (O'Brien, 1999). To accomplish all these, this study will further investigate through theoretical review of various contributions in this line of thinking. But most importantly, this paper will also take cognisance of what the South African (SA) law actually says to protect small businesses from this particular crime (Nagin, 1998). In this regard, a few pieces of legislation will be carefully selected so as to sensitize small businesses about what the legal position currently is. Empirically and to also put more emphasis to this paper, snap interviews have been conducted with bank managers from a few banks in the Gauteng province in SA (Nagin, 1978).

 @ 2013 http://www.ijitr.com All rights Reserved.

III. THEORETICAL FOUNDATIONS

A. What is Identity Theft?

Identity (ID) theft is a form of stealing someone's identity in which someone pretends to be someone else by assuming that person's identity, typically in order to access resources or obtain credit and other benefits in that person's name. Identity, within the context of information systems (IS) criminal activity can be understood as information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual (<http://en.wikipedia.org/wiki/Personally_identifiable_information>). The victim of ID theft (here meaning the person whose identity has been assumed by the ID thief) can suffer adverse consequences if they are held accountable for the perpetrator's actions (Wood, 2007). ID theft occurs when someone uses someone's personally identifying information (PII), like one's name, social security number, or credit card number, without one's permission, to commit fraud or other crimes (Hoofnagle, 2007). The term *ID theft* according to online dictionary available at <http://dictionary.oed.com/cgi/entry/50111220/50111220se23>, was coined in 1964 however, it is not literally possible to steal an identity—less ambiguous terms are identity fraud or impersonation (Baker, 2005). An Automated Teller Machine (ATM) identifies a customer using a card that contains a magnetic strip or smart card chip. The user then provides a personal identification number (PIN) to access account information. Banking is networked, which allows customers to access account information from any ATM in the world (Van Dyke, 2007). Sometimes a fee is charged for using an ATM outside of the customer's banking system. This information is available online at About ATMs eHow.com <http://www.ehow.com/about_5097779_automated-teller-machines.html#ixzz25hHlZhwD> [Retrieved October 17, 2012]. On the other side of things is the ATM being an information system on the part of management.

B. Management Information Systems (MIS)

A MIS provides information that is needed to manage organizations efficiently and effectively (Laudon & Laudon, 2009: 164). MIS are not only computer systems – these systems encompass three primary components: technology, people (individuals, groups, or organizations), and data/information for decision making. MIS are thus distinct from other information systems in that they are designed to be used to analyze and facilitate strategic and operational activities in the organization (CCANB, 1995; Laudon & Laudon, 2010). Academically, the term is commonly used to refer to the study of how individuals, groups, and organizations evaluate, design, implement, manage, and utilize systems to generate information to improve efficiency and effectiveness of decision making, including systems termed *Decision Support Systems*, *Expert Systems*, and *Executive Information Systems* (O'Brien, 1999). Criminals are able to copy [business] information illegally from the magnetic strip (black strip) on the back of the bank card and use this information to steal money (Arora et al., 2004). The device used to copy the information is called a skimming device. Skimming devices can either be handheld or mounted onto an ATM. A later unpublished study by Carnegie Mellon University noted that "Most often, the causes of ID theft is not known," but reported that someone else concluded that "the probability of becoming a victim to ID theft as a result of a data breach is ... around only 2%" (Romanosky, 2008). But then, given all these, what would then be the legal position.

C. SA Legal Stance

Determining the link between data breaches and ID theft is challenging, primarily because ID theft victims often do not know how their personal information was obtained, and ID theft is not always detectable by the individual victims, at least according to a report done for the Federal Trade Commission (FTC, 2006). ID fraud is often but not necessarily the consequence of ID theft. Someone can steal or misappropriate personal information without committing ID theft using the information about every person, such as when a major data breach occurs (Lenard & Rubin, 2005). A US Government Accountability Office study determined that most breaches have not resulted in detected incidents of ID theft, this information is available at <http://www.gao.gov/new.items/d07737.pdf>. This report also warned that "the full extent is unknown". A later unpublished study by Carnegie Mellon University noted that "Most often, the causes of ID theft is not known," but reported that someone else concluded that "the probability of becoming a victim to ID theft as a result of a data breach is ... around only 2%" (Romanosky, 2008). More recently, an association of consumer data companies in SA noted that one of the largest data breaches ever, accounting for over four million records, resulted in only about 1,800 instances of ID theft, according to the company whose systems were breached (available online at <http://pressherald.mainetoday.com/story.php?id=256153>). This paper identifies the following statutes dealing with cybernetic ID crime within the SA context:

 @ 2013 http://www.ijitr.com All rights Reserved.

- Section 85 of the Electronic Communication and Transaction Act (Act 25 of 2002) read with s 86 criminalises the unlawful possession of and utilisation of these devices. Anyone found in unlawful possession of any of such devices can b e prosecuted and be sentenced to an imprisonment or receive a fine.
- Section 15(1) and s 47(A)(1) read with s 80(1)(a) and 83(b) of the Custom and Exercise Act (Act 91 of 1964) stipulate that anyone found being in possession of or who purchases or sells (s 102(1)), imports (38(1) read with s 39 and s 40) or exports such devices can be prosecuted and sentenced to prison.
- Section 155(2)(A) of the Criminal Procedure Act (Act 51 of 1977) stipulates that a receiver of property obtained by means of an offence will be deemed to be part in the offence in question.
- Criminal charges of aiding or abetting an accessory after the fact can also be brought against any person who helps in the illegal copying of card information.

IV. THEORETICAL UNDERPINNINGS

A. Individual ID Protectionism

The acquisition of personal identifiers is made possible through serious breaches of privacy. For consumers, this is usually a result of them naively providing their personal information or login credentials to the ID thieves as a result of being duped but ID-related documents such as credit cards, bank statements, utility bills, checkbooks etc. may also be physically stolen from vehicles, homes and offices, or directly from victims by pickpockets and bag snatchers. Guardianship of personal identifiers by consumers is the most common intervention strategy recommended by the US Federal Trade Commission, Canadian Phone Busters and most sites that address ID theft. Such organizations offer recommendations on how individuals can prevent their information falling into the wrong hands. ID theft can be partially mitigated by *not* identifying oneself unnecessarily (a form of information security control known as risk avoidance). This implies that organizations, IT systems and procedures should not demand excessive amounts of personal information or credentials for identification and authentication (Baum, 2007). Requiring, storing and processing personal identifiers (such as Social Security number, national identification number, drivers license number, credit card number, etc.) increases the risks of ID theft unless this valuable personal information is adequately secured at all times. To protect themselves against electronic ID theft by phishing, hacking or malware, individuals are well advised to maintain computer security, for example by keeping their operating systems and web browser security fully patched against known security vulnerabilities, running antivirus software and being cautious in their use of IT (Givens, 2000). ID thieves sometimes impersonate dead people, using personal information obtained from death notices, gravestones and other sources to exploit delays between the death and the closure of the person's accounts, the inattentiveness of grieving families and weaknesses in the processes for credit-checking. Such crimes may continue for some time until the deceased's families or the authorities notice and react to anomalies, available online at <http://www.nextadvisor.com/identity_theft_protection_services/compare.php>. In recent years, commercial ID theft protection/insurance services have become available in many countries. These services purport to help protect the individual from ID theft or help detect that ID theft has occurred in exchange for a monthly or annual membership fee or premium (FTC, 1998). The services typically work either by setting fraud alerts on the individual's credit files with the three major credit bureaus or by setting up credit report monitoring with the credit bureau. While ID theft protection/insurance services have been heavily marketed, their value has been called into question (Tynan, 2008)

B. ID Protectionism by Organizations

In their May 1998 testimony before the United States Senate, the Federal Trade Commission (FTC) discussed the sale of Social Security numbers and other personal identifiers by credit-raters and data miners. The FTC agreed to the industry's self-regulating principles restricting access to information on credit reports. According to the industry, the restrictions vary according to the category of customer. Credit reporting agencies gather and disclose personal and credit information to a wide business client base. Poor stewardship of personal data by organizations, resulting in unauthorized access to sensitive data, can expose individuals to the risk of ID theft (Pant & Hsu, 1995). The Privacy Rights Clearinghouse has documented over 900 individual data breaches by United States (US) companies and government agencies since January 2005, which together have involved over 200 million total records containing sensitive personal information, many containing social security numbers. Poor corporate diligence standards which can result in data breaches include:

- failure to shred confidential information before throwing it into dumpsters;
- failure to ensure adequate network security;
- credit card numbers stolen by call centre agents and people with access to call recordings;
- the theft of laptop computers or portable media being carried off-site containing

 @ 2013 http://www.ijitr.com All rights Reserved.

vast amounts of personal information. The use of strong encryption on these devices can reduce the chance of data being misused should a criminal obtain them;

- the brokerage of personal information to other businesses without ensuring that the purchaser maintains adequate security controls;
- Failure of governments, when registering sole proprietorships, partnerships, and corporations, to determine if the officers listed in the Articles of Incorporation are who they say they are. This potentially allows criminals access to personal information through credit rating and data mining services.

The failure of corporate or government organizations to protect consumer privacy, client confidentiality and political privacy has been criticized for facilitating the acquisition of personal identifiers by criminals (Iteanu, 2004). Using various types of biometric information, such as fingerprints, for identification and authentication has been cited as a way to thwart ID thieves; however there are technological limitations and privacy concerns associated with these methods as well.

C. Regional Legal Responses

- ***Australia***

In Australia, each state has enacted laws that dealt with different aspects of ID or fraud issues. Some States have now amended relevant criminal laws to reflect crimes of ID theft, such as the Criminal Law Consolidation Act 1935 (SA), Crimes Amendment (Fraud, Identity and Forgery Offences) Act 2009 and also in Queensland under the Criminal Code 1899 (QLD). Other States and Territories are in states of development in respect of regulatory frameworks relating to ID theft such as Western Australia in respect of Criminal Code Amendment (Identity Crime) Bill 2009. On the Commonwealth level, under the *Criminal Code Amendment (Theft, Fraud, Bribery & Related Offences) Act 2000* which amended certain provisions within the *Criminal Code Act 1995*. A person is guilty of an offence if: a) the person does anything with the intention of dishonestly *causing a loss to another person*; and b) the other person is a Commonwealth entity. Penalty: *Imprisonment for 5 years*. Likewise, each state has enacted their own privacy laws to prevent misuse of personal information and data. The Commonwealth *Privacy Act* is applicable only to Commonwealth and territory agencies and to certain private sector bodies (where for example they deal with sensitive records, such as medical records, or they have more than $3 million turnover PA).

- ***Canada***

Under section 402.2 of the *Criminal Code of Canada,*

Everyone commits an offence who knowingly obtains or possesses another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence, is guilty of an indictable offence and liable to imprisonment for a term of not more than five years; or is guilty of an offence punishable on summary conviction.

Under section 403 of the *Criminal Code of Canada,*

> (1) Everyone commits an offence who fraudulently personates another person, living or dead,
>
> (a) with intent to gain advantage for themselves or another person; (b) with intent to obtain any property or an interest in any property; (c) with intent to cause disadvantage to the person being personated or another person; or (d) with intent to avoid arrest or prosecution or to obstruct, pervert or defeat the course of justice. is guilty of an indictable offence and liable to imprisonment for a term of not more than 10 years; or guilty of an offence punishable on summary conviction.

In France, a person convicted of ID theft can be sentenced up to five years in prison and fined up to €75,000 (<http://www.journaldunet.com>). See the Indian Information Technology Act of 2000. Under Hong Kong Laws. Chap 210 *Theft Ordinance*, sec. 16A Fraud

> (1) If any person by any deceit (whether or not the deceit is the sole or main inducement) and with *intent to defraud* induces another person to commit an act or make an omission, which results either-
>
> (a) in *benefit to any person* other than the second-mentioned person; or (b) in prejudice or a substantial risk of prejudice to any person other than the first-mentioned person, the first-mentioned person commits the offense of fraud and is liable on conviction upon indictment to *imprisonment for 14 years.*

Under the *Personal Data (Privacy) Ordinance*, it established the post of Privacy Commissioner for Personal Data and mandate how much personal information one can collect, retain and destruction. This legislation also provides citizens the right to request information held by businesses and government to the extent provided by this law. Punishment for ID Theft under the Indian Information Technology Act 2000 Chapter IX Sec 66C provides that

> Whoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh (The Information Technology Act 2000).

Philippines, known as the 10th heavy users of Facebook and other social networking sites such as

 @ 2013 http://www.ijitr.com All rights Reserved.

Twitter, Multiply and Tumbler has been known as source to various ID theft problems. Identity of those people who carelessly put personal information on their profiles can easily be stolen just by simple browsing. There are people who meet online, get to know each other through the free Facebook chat and exchange of messages that then leads to sharing of private information. Others get romantically involved with their online friends that they tend to give too much information such as their social security number, bank account and even personal basic information such as home address and company address. This phenomena lead to the creation of Senate Bill 52: Cybercrime Prevention Act of 2010 (Full Text of Senate Bill 52 (Proposing the Cybercrime Prevention Act of 2010). Section 2 of this bill states that it recognizes the importance of communication and multimedia for the development, exploitation and dissemination of information but violators will be punished by the law through imprisonment of *prision mayor* or a fine ranging from Php200, 000 and up, but not exceeding 1 million, or depending on the damage caused, or both (Section 7). Legally, Sweden is an open society. The Principle of Public Access says that all information kept by public authorities must be available for anyone except in certain cases. Specifically anyone's address, income, taxes etc. are available to anyone. This makes fraud easier (the address is protected for certain people needing it). To impersonate someone else and gain money from it is a kind of fraud, which is described in the Criminal Code (Swedish:Brottsbalken). In the United Kingdom personal data is protected by the Data Protection Act 1998. The Act covers all personal data which an organization may hold, including names, birthday and anniversary dates, addresses, telephone numbers, etc. Under English law (which extends to Wales but not necessarily to Northern Ireland or Scotland), the deception offences under the Theft Act 1968 increasingly contend with ID theft situations. In *R v Seward* (2005) EWCA Crim 1941 the defendant was acting as the "front man" in the use of stolen credit cards and other documents to obtain goods. He obtained goods to the value of £10,000 for others who are unlikely ever to be identified. The Court of Appeal considered sentencing policy for deception offenses involving "ID theft" and concluded that a prison sentence was required. Henriques J said at para 14: (Blumstein et al., 1978; Acquisti et al., 2006)

" ID fraud is a particularly pernicious and prevalent form of dishonesty calling for, in our judgment, deterrent sentences."

- ***United States (US)***

The increase in crimes of ID theft led to the drafting of the Identity Theft and Assumption Deterrence Act. In 1998, The Federal Trade Commission appeared before the US Senate. The FTC discussed crimes which exploit consumer credit to commit loan fraud, mortgage fraud, lines-of-credit fraud, credit card fraud, commodities and services frauds. The Identity Theft Deterrence Act (2003) [ITADA] amended U.S. Code Title 18, § 1028 ("Fraud related to activity in connection with identification documents, authentication features, and information"). The statute now makes the possession of any "means of identification" to "knowingly transfer, possess, or use without lawful authority" a federal crime, alongside unlawful possession of identification documents. However, for federal jurisdiction to prosecute, the crime must include an "identification document" that either: (a) is purportedly issued by the United States, (b) is used or intended to defraud the United States, (c) is sent through the mail, or (d) is used in a manner that affects interstate or foreign commerce. *See* 18 U.S.C. § 1028(c). Punishment can be up to 5, 15, 20, or 30 years in federal prison, plus fines, depending on the underlying crime per 18 U.S.C. § 1028(b). In addition, punishments for the unlawful use of a "means of identification" were strengthened in § 1028A (Aggravated ID Theft), allowing for a consecutive sentence under specific enumerated felony violations as defined in § 1028A(c)(1) through (11). The Act also provides the Federal Trade Commission (FTC) with authority to track the number of incidents and the dollar value of losses. Their figures relate mainly to consumer financial crimes and not the broader range of all identification-based crimes. If charges are brought by state or local law enforcement agencies, different penalties apply depending on the state. Most states followed California's lead and enacted mandatory data breach notification laws. As a result, companies that report a data breach typically report it to all their customers.

C. Snap Interviews

Snap interviews were conducted with three banks in Gauteng Province in SA. These included, Capitech Bank, ABSA Bank and Standard Bank. The questions posed to these managers were straight forward and to the point, namely; 1) what is the general perception of small business community on ID theft and what is the bank doing to prevent this (Ko & Dorantes, 2006). On answering a question on security, Capitech Bank (13 October 2012) responded as follows:

Seeing that the old card known as 'the Maestro, was clone-able by hackers, we then introduced an anti-clone card system called Debit Master Card (DMC) with a chip on it and the name of the cardholder. Details on the chip were not given as there is a policy that the information on these cards should not be known by the general public. Additional to the Personal Identification Number (PIN), the security set-up on DMC over the counter was described as follows:

- Photo identification keeps the client account secure during branch transactions;

 @ 2013 http://www.ijitr.com All rights Reserved.

- Signature on the card is matched with the one in the system to see if there is a match;
- Fingerprints biometrics then used to access a client's profile;
- The chip on the face of the DMC reveals 'some features' not to be known by general public; and
- The client should then confirm details.

The above information on security was then confirmed by Standard Bank (16 October 2012) and ABSA Bank (17 October 2012) respectively. Summarizing the responses of the three banks the managers generally spoke of almost one and the same thing. These are what were generally indicated:

Anyone who finds any strange device on an ATM or know of person(s) in possession of such a device or devices should immediately contact the police near that area. It can be maddeningly difficult to clear your name, costing hundreds of hours and thousands of dollars. That's why it's important to take steps NOW to make it as difficult as possible for a scammer to victimize you. Take action on these ten tips as soon as possible, and one will tip the scales in one's favour:

- Check your credit report on a regular basis, to see if there is any incorrect information, or accounts you don't recognize;
- Shred your sensitive personal documents before throwing them away. A battery-powered cross-cut shredder can render your banking and credit card information unreadable and costs less than $30. "Dumpster diving" is a favourite, low-tech way by which ID thieves collect bank statements, credit card numbers, Social Security Numbers, and other bits of your identity from your trash.
- Be wary of telephone solicitors asking for personal or financial information to "verify your identity." Common scams involve someone who claims to be from your bank or credit card Company, claiming that there is a problem with your account. If you did not initiate the call, hang up and call the toll-free number on your statement, then ask for the security department;
- Keep important documents, such as tax returns, birth certificates, social security cards, passports, life insurance policies and financial statements secure in your home. A fireproof safe is a good idea, but remember to bolt it to the floor or hide it well;
- Make sure no one is looking over your shoulder when you enter your debit card's Personal Information Number (PIN) at ATM or point-of-sale terminal. I recommend the "two finger method" where you point two fingers at the ATM keypad, but only press with one. This makes it nearly impossible for someone nearby to discern your PIN while you're entering it;
- Memorize PINs, account numbers, and passwords; do not write them down. And for heaven's sake, do not put such data on scraps of paper kept in your wallet, purse, or laptop case!
- Get blank checks delivered to your bank branch, not to your home mailbox from which they may be stolen. On a similar note, eliminate junk mail which may contain "convenience checks" and credit card offers that can also be intercepted from your mailbox;
- When you order a new credit or debit card, mark the calendar and follow up promptly if it does not arrive within 10 business days. Ask the card issuer if a change of address request was filed, and if you didn't do it, hit the panic button; and
- Don't give your Social Security Number to any business just because they need a "unique identifier" for you. Instead, ask if you can provide alternate proofs of identity, such as your driver's license or birth certificate.

Consider placing Fraud Alerts with the major credit bureaus, so new accounts cannot be opened without your knowledge. Call Equifax (800-525-6285), and they will pass along the request to both Experian and Trans Union. Fraud alerts expire after 90 days, so you can repeat the process quarterly, or lock down your credit file with a Credit Freeze. A freeze is permanent and free (in most US states, though) but it may interfere with loans applications, employment screening, signing up for utility or phone service, new insurance policies, and other transactions. One will also need to contact each credit bureau (<http://www.freeze.equifax><http://experian.com/consumer/security_freeze.html> and <http://www.transunion.com/corporate/personal/fraudidentityTheft/fraudPrevention/securityFreeze.page>) to request the credit freeze.

V. IMPLICATIONS AND CONCLUSION

A business may be considering Life-Lock or a similar ID theft protection service. Although this can be helpful, no business can guarantee that ID theft will never happen. These services monitor business bank account, and look for suspicious online activity done in the business name. They will alert the business or an individual if they spot

 @ 2013 http://www.ijitr.com All rights Reserved.

any red flags and promise to help repair the damage. But because of lawsuits filed by the credit bureaus, Life-lock can no longer place fraud alerts on an individual or business behalf. Looking abroad, all identity protection services are barred from offering ID theft insurance coverage to residents of New York (Citi Bank, 2012). Since one would have to manage fraud alerts or a credit freeze on one's own, and because there is so much one can do on one's own to protect against ID theft, I don't see much value in these services. ID theft is one of the most traumatic non-violent crimes to which one can fall victim. When a crook uses one's or business good name to commit fraud or robbery, the impact on one's reputation or that of the business, employability, and credit is severe and can last for years. One may even find oneself arrested for crimes one did not commit. So it's important to protect one against ID thieves. The telltale signs that one's identity has been stolen can be subtle and go unnoticed for months, even years. Inexplicable charges on the business credit card bill, including that of an individual, may be chalked up to clerical errors. Letters from creditors one have never heard of and certainly never did business with may still be ignored. But eventually, an enormous credit card bill, legal papers or police show up at one's door. You are denied a mortgage or a job. Then the real nightmare of proving "I didn't do it" begins. The same goes for businesses on insolvency notices, but most importantly, a few tips that the three banks have provided are hoped to assist small businesses forming part of their MIS and individuals to always be on their alert each time they visit the ATM and/or the bank counters for transactions other than cell-phone or telephone banking.

VI. REFERENCES

[1] Acquisti, A., Friedman, A. & Telang, R. (2006). Is There a Cost to Privacy Breaches? An Event Study, Fifth Workshop on the Economics of Information Security, 2006.

[2] Arora, A., Telang, R. & Xu, H. (2004). Optimal Policy for Software Vulnerability Disclosure. *The Third Annual Workshop on Economics and Information Security* (WEIS04).

[3] Baker, Bob (2005). King of Pop impersonator star of E! Trial re-enactment. *The Seattle Times*. <http://seattletimes.nwsource.com/html/nationworld/2002195262_jacko03.html> [Retrieved September 28, 2012]

[4] Baum, K. (2007). Identity Theft, 2005. *Bureau of Justice Statistics Special Report NCJ 219411*, November 2007.

[5] Blumstein, A., Cohen, J. & Nagin, D. (1978). Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime Rates, Report of the Panel of Deterrence and Incapacitation. *National Academy of Sciences*, Washington, D.C.

[6] Carpenter, B. (2012). *Bank Card Scam Using Texting to Phish Data.* Pronews 7 and ConnectAmarillo.com.

[7] Comptroller of the Currency Administrator of National Banks (1995). Management Information Systems. Comptroller's Handbook May 1995.

[8] Criminal Procedure Act 51 of 1977. Government Gazette, South Africa.

[9] Custom and Exercise Act 91 of 1964. Government Gazette, South Africa.

[10] Electronic Communication and Transaction Act 25 of 2002. Government Gazette, South Africa.

[11] Federal Trade Commission – 2006 Identity Theft Survey Report, p.4. <http://www.gao.gov/new.items/d07737.pdf. Retrieved 22 September 2010> [Retrieved September 24, 2012]

[12] Giles, J. (2010). Cyber Crime Made Easy. New Scientist, 205.2752 (2010): 20-21. *Academic Search Premier*. EBSCO. Web. 3 Oct. 2010.

[13] Givens, B. (2000). Identity Theft: How It Happens, Its Impact on Victims, and Legislative Solutions. *Written Testimony for U.S. Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information*, July 12, 2000.

[14] Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known," *Harvard Journal of Law and Technology*, Vol. 21.

[15] Identity Theft Deterrence Act of 2003.

[16] Iteanu, O. (2004). Usurpation D'identité: La Loi Ou la Technique Pour se Protéger? Nouvelles Offres D'emploi.

[17] Ko, M. & Dorantes, C. (2006). The Impact of Information Security Breaches on Financial pPerformance of the Breached Firms: an Empirical Investigation. *Journal of Information Technology Management*, Volume XVII, Number 2.

[18] Laudon, K. C. & Laudon, J. P. (2009). *Management Information Systems: Managing the Digital Firm* (11th Ed.). Prentice Hall/CourseSmart.

[19] Laudon, K. P. & Laudon, J. P. (2010). *Management Information Systems: Managing the Digital Firm.* (11th Ed.).

 @ 2013 http://www.ijitr.com All rights Reserved.

Upper Saddle River, NJ: Pearson Prentice Hall.

[20] Larry, W. (2010). *Plastic Money to Replace Paper Currency in Canada.* Available online at <http://pressherald.mainetoday.com/story.php?id=256153>. [Dead Link].

[21] Lenard, T. M. & Rubin, P. H. (2005). Slow Down on Data Security Legislation." *Progress Snapshot 1.9*. The Progress & Freedom Foundation.

[22] Nagin, D. (1978). General Deterrence: A Review of the Empirical Evidence," in Alfred Blumstein, Jacqueline Cohen, and Daniel Nagin (eds.), Deterrence and Incapacitation: Estimating the Effects of Criminal Sanctions on Crime (Washington, D.C.: National Academy of Science.

[23] Nagin, D. (1998). Criminal Deterrence research at the outset of the twenty-first century. *Crime and Justice*, Volume 23.

[24] O'Brien, J (1999). *Management Information Systems – Managing Information Technology in the Internetworked Enterprise*. Boston: Irwin McGraw-Hill.

[25] Oxford English Dictionary online (2007). Oxford University Press. September 2007. <http://dictionary.oed.com/cgi/entry/50111220/50111220se23>. [Retrieved September 27, 2012]

[26] Pant, S. & Hsu, C., (1995). Strategic Information Systems Planning: A Review. *Information Resources Management Association International Conference*, May 21–24, Atlanta.

[27] Prepared Statement of the Federal Trade Commission on "Identity Theft", Subcommittee on Technology,Terrorism and Government Information, Washington, D.C. May 20, 1998.

[28] Romanosky, S. (2008). Do Data Breach Disclosure Laws Reduce Identity Theft? *Heinz First Research Paper*. heinz.cmu.edu. [http://www.heinz.cmu.edu/research/241full.pdf>. [Retrieved September 24, 2012]

[29] Senate Bill 52 Proposing the Cybercrime Prevention Act of 2010, Full Text.

[30] Tynan, D. (2008). Identity-Theft Protection: What Services Can You Trust? *PC World*.

[31] Van Dyke, J. (2007). Reading behind the lines: How Identity Fraud Really Happens. *Javelin Strategy & Research,* 2007.

[32] Wood, D. (2007). GAO-07-737 Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown. *Government Accountability Office*.

IJITR