SOUTH AFRICAN ONLINE BANKING: WHO CARRIES THE RISK?

Anna Granova & JHP Eloff, ICSA Research Laboratory, Department of Computer Science, University of Pretoria

Abstract

Today, Internet fraud occurs more and more frequently, and its devastating effects for organisations, such as banks, as well as their clients constitutes a continuous nightmare for all parties concerned.

With regard to criminal and civil liability of the bank as well as that of the customers, the role the Information Security Policy plays in an organisation, and the possibly binding force of information security policies, it is clear that unless the organisation takes all the necessary steps to educate its clients, it stands a risk of paying hefty damages for loss of money online.

Keywords

- Online banking / banking online;
- Liability of a bank;
- Internet law;
- ABSA;
- Identity theft;
- Internet banking contract;
- Internet and risk.

1. Introduction

The advent of the Internet revolutionised many industries, including banking, by eliminating the need of physically going to the specific organisation and filling in paper forms in order to perform a transaction. Today, many of these operations can be done online. The current increasingly "faceless" interface of the manner of doing business has done away with prerequisites like producing of an I.D. document or

inserting a card, replacing all of that, for the purposes of identification, with a username and password.

Therefore, apart from the obvious benefits of the system, there are collateral risks associated with the absence of personal contact. The most dangerous of all of them is the reduced risk for, and effort required on the part of, "would-be-thieves" for "passing off" as legitimate clients. A couple of years ago, such a delinquent would have to forge not only the signature but also the whole identification document, while today much easier ways of defrauding are available to them.

People have always banked mostly out of convenience and security, associated with holding money at financial institutions. The sense of security, in particular, came out of the assumed responsibility by the bank to verify the identity of the person who requested access to the money in question.

This is not to say that the customer would not under any circumstances be responsible for loss of money. Thus, should the customer fail to protect the PIN and or loose the ATM card, for example, and fail to promptly notify the bank about it, he/she will be found (at least by the court of law) negligent and, therefore, responsible for the loss.

This paper is, therefore, limited to what are known to be the "legal implications" of the above-mentioned situations. For ease of reference and to provide a factual basis for this discussion, the recent challenges ABSA bank, one of the largest banking institutions in South Africa, had to face in the context of a developing country and its legal system, will be used as an example.

Keeping in mind the principle that customers would only carry the risk to the extent he/she has contributed to it (whether intentionally or negligently),[1] and the fact in this specific instance that they were neither,[2] the this paper focuses on the following inter-related aspects of this incident, which may have far-reaching implications for businesses, who use the Internet as a tool:

[1] *Minister of Safety and Security v Van Duivenboden* 2002 (6) SA 431 (SCA) para 12 at 441E-442A.
[2] There was definitely no intention to provide the information to the hackers (Johns L (2003) "Police arrest suspected ABSA hacker and recover cash" 27 July 2003 *Sunday Trubune* 8). As for possibility of negligence see para 3.2.2.2 below for discussion.

1. Criminal and civil liability of the bank as well as that of the customers;
2. The role the Information Security Policy plays in an organisation;
3. Finally, the binding force of information security policies and possible transfer of risk and accountability from the organisation to the customer.

Before addressing the above, it is necessary to refer to the relevant facts of the ABSA incident in order to provide a background for the remainder of the paper.

2. Facts

ABSA bank has provided Internet banking service to its clients for several years. In a recent "identity theft" incident, ten ABSA Internet banking clients cumulatively lost R530,000 due to unauthorised online Internet transactions performed on their accounts, all of which were carried out between May and July 2003.[3]

Contrary to popular belief, the loss of money could not have been attributed to an act of "hacking" since the Spyware software in question, also known as a Trojan, was attached to an email, which unsuspecting customers were enticed to open on his/her computer. Thereafter, the Trojan recorded all key strokes and secretly e-mailed this information to the perpetrator, who, in turn, logged into his victim's online Internet banking accounts and transferred money to selected organisations as payment for goods purchased, or another bank account for the purposes of withdrawal.[4]

At the time of the incidents, according to research conducted by Trust Online,[5] ABSA bank had achieved only 63% compliance[6] with the Electronic Communications and Transactions Act ("the ECT Act"),[7] the new piece of legislation dealing with the Internet. Poor compliance with the Act in all probability did not cause the breach of

[3] Johns L (2003) "ABSA account hacking suspect to appear in court tomorrow" *Sunday Independent* 27 July 2003 1; Johns L (2003) "Police arrest suspected ABSA hacker and recover cash" *Sunday Tribune* 27 July 2003 8.
[4] Naidoo K (2003) "Seven seconds to crack bank internet security" August 2003 *Leader* 2.
[5] A company that certifies websites, www.trustonline.co.za [although it does not seem to function any longer].
[6] Opperman I (2003) "ABSA – 'kraker' steel klient-inligting" *Beeld* 27 July 2003 1.
[7] 25 of 2002.

security, but it was rather the lack of effort, most probably due to ignorance, on the part of the customers to take appropriate steps to protect the confidentiality of account log-in information such as user names, passwords, PIN's. The same way that the banks strongly advise customers to guard both the credit/debit cards and the PIN's, so should be the case in respect of usernames and passwords.

Although one can try to assign all the liability to the consumer, as attempted by ABSA by claiming that its security was not compromised,[8] there are sound arguments surrounding this type of scenario why the liability and accountability rather rests with the bank. The reason for this will become apparent from the forthcoming discussion.

3. Responsibility and liability

The South African legal system has two main components: common law and legislation. The perpetrator is doubtless liable under both so-called regimes: criminally for theft of money and fraud in terms of common law and offences as prescribed in terms of the ECT Act[9] and Interception and Monitoring Prohibition Act.[10] Furthermore, there is also the possibility of civil liability for his/her action on the basis of delict as will be seen shortly.

The question that arises is whether, and to what extent, the other two parties affected, namely the business (a bank in this case study) and client have to share the responsibility for the incident and assume relevant liability (whether civil or criminal) that has arisen from the incident, whether in monetary or other terms (imprisonment should the state pursue a criminal case).

3.1 Criminal Liability: Fraud

Fraud is defined as "the unlawful and intentional making of a misrepresentation which causes actual prejudice or which is potentially prejudicial to another".[11]

[8] Clayton C (2003) "Your PC, your responsibility, say banks" *Saturday Star* 26 July 2003 3.
[9] In terms of section 86.
[10] 127 of 1992.
[11] Snyman CR *Criminal Law* (2002) 4th ed 520; *S v Campbell* 1991 (1) SACR 503 (NM) at 505; See also *S v Van den Berg* 1991 (1) SACR 104 (T) at 106.

Applying the above definition to the facts at hand, it is clear that the bank may have misled the public in respect of the security of Internet banking, and perhaps created a false sense of security pertaining to online transactions. Lack of campaigns warning consumers of potential risks may further support the proposition that there was misrepresentation. The customer, at least, needs to be educated as to the nature of and risks associated with "passwords," "usernames" and "identity theft". Furthermore, clear default instructions as to what steps to take if either password or username are even suspected to have been stolen need to be issued.

The obvious question, "Who defrauded the customer?" does not have only one correct answer. On the construction of this case, one thing is clear – ABSA was not free from criminal liability on the basis of fraud.

Furthermore, the requirements of prejudice and unlawfulness are also present on the facts: actions or rather non-actions on the part of ABSA which led to loss of more than R500,000 may not, under no circumstances, be argued to be lawful or not prejudicial to the clients.

It is only the final requirement of intention that may pose difficulties for substantiating and attributing guilt on a charge of fraud to ABSA. The only indication that there has been such an intention is non-disclosure, the possible intentional concealment of information concerning the existence of threats posed by Spyware, a fact undeniably known to ABSA prior to the incidents recently experienced. It is due to existence of intention not to disclose (the motive for which is irrelevant) that the bank may be prosecuted for fraud.[12]

The final consideration is of a practical nature, in that the desirability of criminally punishing a corporate body has always been a matter of controversy.[13] It is on this

[12] In *S v African Bank of South Africa Ltd and Others* 1990 (2) SACR 585 (W) at 646, the Court clearly stated:

> "That a failure to disclose can constitute fraud is well settled."

[13] Snyman CR *Criminal Law* (2002) 4th ed 249.

ground that the prosecution of the company may be stayed, but this does not imply that the company is not liable.

3.2 Civil Liability

There are two legal grounds upon which the bank could be found liable: delict and contract.

3.2.1 Delict

Delict can be defined as a "civil wrong to an individual for which damages can be claimed as compensation and for which redress is not usually dependent on a prior contractual undertaking to refrain from causing harm."[14]

Liability of a company on this basis includes, but is not limited to, deceptive and fraudulent business practices and false advertising. Where a court of law might not find enough evidence for the company to be convicted for fraud in criminal proceedings, the lighter burden of proof (on the balance of probabilities as opposed to beyond reasonable doubt in criminal cases) may very well lead to hefty damages payable to the consumer.

In practice, fraud may be either a delict or a crime, depending on its seriousness.[15] To be considered a delict, fraud should involve a breach of community standards, also known as "legal policy"[16] which obviously varies from one context to another.

It is appropriate at this stage to mention that standards like ISO17799 cannot be regarded as those of the community, because the standards of the community consist of the generalised idea of what an ordinary person on the street accepts as acceptable behaviour. Since ISO17799 is very specialised and can be argued not even to be

[14] Burchell J (1993) *Principles of Delict* 9.
[15] Hofman J *et al* (1999) *Cyberlaw: A Guide for South Africans Doing Business Online* 125.
[16] In *Minister of Safety and Security v Van Duivenboden* 2002 (6) SA 431 (SCA) para 16 at 444B/C-C/D it was held that:

> *"The question to be determined is one of legal policy, which must of necessity be answered against the background of the norms and values of the particular society in which the principle is sought to be applied."*

familiar to all specialists in the IT industry, it would be unrealistic to expect others to possess it as part of their general knowledge. Therefore, ISO17799 is only an industry standard and not that of the community.

Further, we are in South Africa, all the unique circumstances we live in, such as low computer literacy, general ignorance of Internet-related security issues, coupled with reliance on information that comes from an authoritative body, such as a banking institution or a government department, all have to be taken into consideration.

In addition, negligence is used as a standard applicable to the assessment of financial loss in such cases. Added to everything already said in this respect, in order to hold the bank liable, the latter's conduct should fall below the legal convictions or feelings of the community,[17] which are not (however unfortunately) rooted in industry codes like ISO1799.

Many banks claim to provide secure online banking facilities but remain silent on the necessity and therefore obligation on the part of the consumer to ensure the security of his/her computer (whether it is in the form of updated antivirus or otherwise), and therefore they failed to fulfil their legal duty of care and as stated above, the high standard of care in South African context.

Further, the bank is most probably liable on the basis of *acquilian* action since the damage incurred by the client was, at least, foreseeable in that the existence of Spyware has been known for more than 15 years.[18]

At the time of the online disaster, it was neither possible for ABSA to raise any of the legal defences, whether that defence was voluntary assumption of risk by the customer, contributory negligence or mitigation of loss; as the consumers could not have been expected to act any differently than the manner in which they did under the circumstances.

[17] *Costal States Trading, Inc. v Shell Pipeline Corp* 573 F.Supp. 1414.
[18] Clayton C (2003) "Your PC, your responsibility, say banks" *Saturday Star* 26 July 2003 3.

Finally, since 1979 South African courts have recognised a broad principle of liability for negligent misstatements,[19] especially where a person does not have any expertise in the area concerned, which derived from professional negligence, where

> *"anyone, not just a person in the traditional categories of advisers, who gives advice with the expectation that it will be acted upon will be liable for foreseeable economic loss consequent upon the giving of the advice negligently."*[20]

It is clear that ABSA, by marketing its online banking facilities through distribution of free software, acted as an educator in the area of Internet banking in general. Thus, in order to avoid liability, it has to be more proactive, as it has been since the incidents, and must continue educating its customers in respect of possible information security threats, and corresponding precautions they will have to take to prevent similar incidents from occurring.

So far, ABSA has placed relevant information in respect of its use of encryption technology, access numbers and PIN's, and passwords on its website,[21] and introduced features like "online keypad on the logon screen", limiting a number of opportunities to enter the PIN correctly to three.

Furthermore, an option to receive a unique code (Random Verification Number) via e-mail or SMS for purposes of controlling creation of a valid beneficiary and one-year offer for free antivirus software are definitely steps forward in addressing the situation.

The standard of care required by the South African law goes as far as to require that a person or organisation has done everything reasonably expected from him by the society at large. Therefore, any organisation undertaking the measures as mentioned above, should be confident that it is on its way to comply with such standard of care and limit and/or eliminate any liability for damages *vis-à-vis* its customers.

3.2.2 Contract

[19] *Administrateur, Natal v Trust Bank van Afrika Bpk* 1979 (3) SA 824 (A).
[20] *Hedley Byrne & Co v Heller & Partners Ltd* [1964] A.C. 465, [1963] 2 All E.R. 575.
[21] <www.absa.co.za> accessed on 18 May 2004.

It is well known that most of relationships between an organisation and clients are incorporated into a written contract. With respect to banks, contracts become very central to the bank-client relationship[22] and very often there is more than one document involved. It must, however, be noted that internal Information Security Policies of a bank are not part and parcel of the contract, unless drafted for that specific purpose. As transpires from practice, such policies are "coined" into "Terms and Conditions" and therefore given a formal name therefore it excludes any similar document, which caters for relationships between the bank as an entity and its employees.

When it comes, however, to obligations that arise from the bank-client relationship, there are two important aspects at play: implied warranties and misrepresentation.

3.2.2.1 Implied Warranties

Implied warranties are warranties that exist without an express term to that effect in the contract. The reason for the so-called "reading-in" of contracts, is that it is in the public interest for the government to protect some crucial rights of consumers and promote "fair dealing" in the market.

Therefore, sometimes, through representation and prevailing circumstances, implied (unwritten) warranties become part of the contract between the client and the bank. In that case, any violation of such a warranty would attract civil liability, and the bank, being the party making the promises, becomes liable for damages if it fails to honour them.

There are two reasons for this: firstly, the assumption that it is reasonable for the customer to assume that their money is safe in the bank, is sound and therefore valid.

[22] Cranston R (2002) *Principles of Banking Law* 2nd ed 133.

Secondly, the assumption in law that he who drafts the contract owes a heavier duty towards the other party,[23] is also applicable in this case. It is simply impossible to imagine a client requesting the bank to change the terms and conditions of the contract in accordance with his or her wishes, whereby he would be have a say in the matter.

Therefore, it is essential for the bank to ensure that the customer is aware of everything with to the contract. It is important to add that in a pre-online banking environment, the customer was made aware that both the ATM card and corresponding PIN (password) had to be kept secure by the customer himself. Also, if one wanted to withdraw money at a branch, an I.D. document had to be presented and a valid signature provided, before any money would be released.

Today, however, the bank will only be on the safe side if the same type of information is constantly reinforced, thereby reducing the likelihood of a reasonable consumer being able to plead breach of contract as a defence.

3.2.2.2 Misrepresentation

Another factor that has obviously vitiated the contract that existed between ABSA bank and it clients is misrepresentation.[24]

At the time of the ABSA incidents, the contract between the client and the bank only stated that the former were "not to *give* or *make available* in any way his personal Log-in ID and password to any other person for such person's use" and the bank would not be liable "unless the user is able to *prove* that the person has obtained the Log-in ID and password due to Absa's *negligence* or due to internal fraud in Absa."[25]

As already discussed earlier, negligence in terms of failure to act in such reasonable manner as expected by the community, while on the facts of the case the clients did

[23] This rule is also known as *contra proferentem* rule; See for discussion Van der Merwe S *et al* (1994) *Contract: General Principles* 223; *Cairns (Pty) Ltd v Playdon & Co Ltd* 1948 (3) SA 99 (A) 122-5.
[24] Kerr AJ (2002) *The Principles of the Law of Contract* 6th ed 295.
[25] Para 4.1.2 of the *Term and Conditions for ABSA Internet Access* available at <http://web.archive.org/web/20030608203829/www.absa.co.za/Individual/0,2999,2127,00.html> accessed on 18 May 2004.

not "give" or "make available" their usernames and passwords, but they were, in actual fact, proven to have been stolen.

Furthermore, there was no legal basis for ABSA to invoke paragraph 4.4 of that particular contract, which stated that "[t]he user agrees to conform to generally acceptable Internet etiquette ('netiquette')",[26] due to the fact that this clause is so vague, it would be found by any court of law to be invalid. Therefore, all ten clients were entitled to sue for damages in any case.[27]

Even in the absence of misrepresentation (whether intentional or negligent), there remained a duty to disclose since the circumstances were such that "frank disclosure [is] clearly called for".[28] In other words, persons banking with ABSA online would not have known about the intricacies of making using of web based services and the associated risks, without the bank disclosing it to them.

Nowadays, of course, all the banks in South Africa have drawn so called "terms and conditions", which are readily available for perusal on their respective websites and one may not proceed to the next step of registration for Internet banking without accepting them.[29] Although a similar system was in place before,[30] the wording, format and layout used today is more user-friendly and the contract *per se* is easier to read, the making the customer's obligations easier to understand.

Although all of the above institutions have stated in their contracts that they are not liable for any damage whatsoever, this is in conflict with, and therefore overridden by the current legislation in South Africa. It is submitted that the ECT Act read in

---

[26] Para 4.1.2 of the *Term and Conditions for ABSA Internet Access* available at <http://web.archive.org/web/20030608203829/www.absa.co.za/Individual/0,2999,2127,00.html> accessed on 18 May 2004.

[27] Christie RH (2001) *The Law of Contract in South Africa* 4th ed 346.

[28] Kerr AJ (2002) *The Principles of the Law of Contract* 6th ed 301; *Gollach & Gomperts (1969) (Pty) Ltd v Universal Mills & Produce Co (Pty) Ltd and Others* 1978 1 SA 914 (A) at 924A-B.

[29] Examples of such can, for example, be found on https://www.nedbank.co.za/website/content/forms/form.asp?FormsId=73 accessed on 05 May 2004 and https://e91.absa.co.za/aia/registration/frameset.jsp accessed on 09 May 2004.

[30] http://web.archive.org/web/20040519041819/https://e91.absa.co.za/aia/registration/frameset.jsp accessed on 19 May 2004

conjustion with the King II Report on Corporate Governance, places the responsibility of ensuring security on the web site owner.[31]

Therefore, notwithstanding the conservative state of the South African legal system, there are some solid requirements that every organisation has to comply with in order to continue to prosper within the given legal regime.

4. Conclusion

Although the question of reimbursement as pertaining to the ABSA case has been settled, cases involving fraud and consequential damages are almost certain to arise in the future.

In the light of the above, it is clear that an organisation will always carry the risk and be liable for damages or loss that result from an incident similar to that involving ABSA unless it can prove that it has identified all potential risks and took "all reasonable steps to avoid the risk or at least limit the consequences."[32] The client will only bear the risk if the organisation can prove that he/she has disregarded explicit instructions it supplied to him/her for the purposes of reducing the risk.

The important lesson that should have been learnt here is that IT security has to be given a high priority when providing online services to your customers. Failing to do so could expose an organisation to recurring, yet avoidable liabilities.

Therefore, the business sector is faced with an exciting opportunity to strengthen its vigilance as a business, by actively participating in the education of Internet users, and through achieving compliance with relevant laws and regulations.

[31] Unknown (2002) "SA bank Web sites not safe and compliant - survey" 02 October 2002 *E-Briefs* as appear on http://www.legalbrief.co.za/view_1.php?artnum=7419 accessed on 09 May 2004.
[32] Unknown (2003) "Who's liable for online bank thefts?" 30 October 2003 available at http://www.legalbrief.co.za/view_1.php?artnum=12855 accessed on 18 May 2004.