CONSUMER PROTECTION MEASURES FOR ERRONEOUS OR UNAUTHORIZED INTERNET PAYMENTS: SOME LESSONS FROM THE EUROPEAN UNION?

1 Introduction

The increase in cyber malls or internet shops presents consumers with a magnitude of goods, including digitized goods and information to choose from. In purchasing these commodities, the internet, in particular, offers the consumer various payment possibilities, such as credit card and online fund transfers to third parties. However, these payment instruments are not flawless. Errors may occur whilst the consumer is making such payment, the system may malfunction or unauthorized payments may be made.

The aim of this analysis is to ascertain whether the existing law has measures that would be wide enough to protect a consumer in these instances. The position in South Africa is evaluated against this background and compared with the position in the European Union.

2 The risks

The success of electronic commerce is dependent on the availability of online payment mechanisms. Fear about the security of online payment methods is the area of greatest concern to consumers who are considering making an online transaction.

The risk to consumers of using credit cards is twofold. Firstly, information such as credit card details could be intercepted on route to the trader and used improperly by a third party. Secondly, the business itself may use the information improperly. The increasing effectiveness of security measures such as encryption should help increase consumer confidence in the safe handling of payment information. However, identifying disreputable traders who misuse payment information is a more difficult problem for consumers.

Credit card companies have been active in seeking to minimize fraud and to protect their clients in the internet environment. One such initiative is the Secure Electronic Transactions (SET) system. Another consumer protection initiative operated by credit card companies involves “chargebacks”. This allows a credit card holder who paid for goods or services using a credit card to dispute certain or all aspects of the transaction through the payment card issuer. Where disputes occur, chargebacks allow consumers to bypass legal proceedings and may also encourage the co-operative resolution of

consumer complaints by traders wishing to retain their status with the credit card company. Chargebacks can help to increase consumer confidence by allowing consumers to place greater reliance on the trader's representations. However, in the absence of these initiatives, the risks mentioned earlier remain.

Moving payments such as electronic funds transfers ("EFTs") onto the internet remains troubling since it introduces additional security concerns and exposures. The internet exposes EFT activity to more than just threats to steal money. An antagonist can launch a denial-of-service attack that leaves the funds safe, but stymies the system so that the user cannot use it. This can be devastating to a financial business such as stock brokerages whose business is built on the reliability of their payments. The real problem with the internet is, therefore, not only security, but also reliability, although not the subject of this enquiry. In addition, matters are complicated by the anonymity of the perpetrator and the fact that no paper trail is left.

However, the question remains whether or not a consumer is adequately protected against some of these risks and unauthorized, fraudulent or erroneous payments over the internet. For the purpose of this note no distinction is made between whether a credit card or EFT is used.

3 Legal and policy developments in the European Union

The law seeks to address the problem of loss allocation or consumer protection in different ways. Sometimes legislation supplemented by common law rules applies (see *eg*, the principles of mandate and unauthorized payment in cheques in Lawack-Davids *Aspects of Internet Payment Instruments* (unpublished LLD thesis (UNISA) 2000) 151) and sometimes the problems, which may arise in connection with some payment instruments, are covered by the terms and conditions of use relating to the payment instrument.

The European Commission Recommendation of 30 July 1997 concerning transactions by electronic payment instruments and, in particular the relationship between issuer and holder, only governs certain forms of payment (see *Commission Recommendation* 97/489EC which updated *Commission Recommendation* 88/590/EEC OJ L317/55) of 17 November 1988 concerning payment systems and in particular the relationship between cardholder and card issuer). This Recommendation was applicable in its entirety to all transactions involving instruments that allow remote access to the holder's account such as transfers of funds, other than those ordered and executed by financial institutions, effected by means of an electronic payment instrument. It also included cash withdrawals by means of an electronic payment instrument and the loading and unloading of an electronic money instrument, at devices such as cash-dispensing machines and automated teller machines (ATMs).

This Recommendation, therefore, included in particular, payment cards (whether credit, debit, deferred debit or charge cards) and phone- and home-banking applications (see Poullet and Vandenberghe *Telebanking, Teleshopping and the Law* (1988) 12ff; Vergari and Shue *Checks, Payments and Electronic Banking* (1988) 514ff; Lawack *Electronic Payment System in South African Law* (unpublished LLM dissertation (UPE) 1997) 127*ff* for more detail on home banking). The Recommendation did not apply to transactions effected by means of an electronic money instrument, except where the electronic money instrument is used to load and unload value through remote access to the holder's account (Article 1). To the extent that an electronic money instrument is not used in this manner, it was (and still is) dealt with by a separate Directive that deals with the supervisory issues relating to electronic money (see the European Union Directive 2000/46 on the *Taking Up, Pursuit of and Prudential Supervision of the Business of Electronic Money Institutions Official Journal of the European Communities* L 275/39. See also the *Proposal for a European Parliament and Council Directive on the Taking up, the Pursuit and the Prudential Supervision of the Business of Electronic Money Institutions* repealed by Directive 2009/110/EC of 16 September 2009). The Recommendation did, likewise, not apply to payments by cheques and the guarantee function of certain cards in relation to payments by cheques (cheque cards) (on the cheque card see Lawack-Davids *Internet Instruments* 142).

There have been a few significant legal and policy developments in the European Union since the above Recommendation. These developments include the European Commission Directive concerning the distance marketing of consumer financial services which covers all financial services liable to be provided at a distance (Directive 2002/65/EC of 23 September 2002). A financial service is defined as any service of a banking, credit, insurance, personal pension, investment or payment nature (Article 2). A "means of distance communication" is defined as "any means which, without the simultaneous physical presence of the supplier and the consumer, may be used for the distance marketing of a service between those parties. It would appear that the internet could be a "means of distance communication" as this definition seems sufficiently wide to include the internet. With specific reference to payment by card, Article 8 provides that member states have to ensure that appropriate measures exist to allow a consumer to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts and in the event of such fraudulent use, that such consumer be re-credited with the sum paid or have this sum returned. There is nothing in the Directive that suggests that card payment via the internet would be excluded from this provision. The Directive contains no further particular provisions dealing with unauthorized payment and/or loss allocation relating to other forms of payment.

Despite the above legal framework, it was felt that the measures were fragmented and insufficient. The co-existence of national provisions and an incomplete Community framework gave rise to confusion and a lack of legal

certainty. To this end, the European Commission embarked on a consultation process to advocate for a New Legal Framework for Payments in the Internal Market (see Communication from the Commission to the Council and the European Parliament concerning a New Legal Framework for Payments in the Internal Market (Consultative Document of 2 December 2003 (COM (2003) 718 final). The consultation process was followed by a Proposal for a Directive (Proposal for a Directive of the European Parliament and of the Council on Payment Services in the Internal Market COM (2005) 603 final), which would repeal all the existing legislation, *inter alia*, the Recommendation discussed above. The result was Directive 2007/64/EC of 13 November 2007 on payment services in the internal market. This Directive applies to payment services provided within the European Community. The definition of a "payment service" refers to "any business activity listed in the Annex to the Directive (see Article 4). Included in the list of "payment services" in the Annex, is the execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier or goods and services. If the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services, such transaction would not be a "payment service" as defined (see the negative scope in Article 3(l)). Since payment over the internet would fall within this definition of the internet service provider acting only as an intermediary (and not as a party to the transaction), such payment would be considered a "payment service" in accordance with the Directive. A "payment service user" means a natural or legal person making use of a payment service in the capacity of either a payer or payee, or both (see Article 4 (10) – hereinafter "PSU"). A "payment service provider" (hereinafter "PSP") means anybody referred to in Article 1(1) and legal and natural persons benefitting from the waiver under Article 26. These bodies referred to in Article 1(1) include the following six categories of payment service provider:

(a) Credit institutions;

(b) electronic money institutions;

(c) post office gyro institutions which are entitled under national law to provide payment services;

(d) payment institutions in terms of the Directive;

(e) the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities; and

(f) member states or their regional or local authorities when not acting in their capacity as public authorities.

PSPs may benefit from the waiver of certain provisions of the Directive which member states may allow when the average of the preceding 12 months' total amount of payment transactions executed by the PSP,

including its lawful agents, does not exceed EUR 3 million per month and none of the natural persons responsible for the management or operation of the business has been convicted of offences relating to money laundering or terrorist financing or other financial crimes (Article 26(1)(a) and (b)).

Title IV of the Directive describes the rights and obligations in relation to the provision and use of payment services. With specific reference to the current enquiry, it has to be noted that there are provisions in Chapter 2 of Title IV dealing with the duties of the PSU and PSP, unauthorized payment and non-execution or defective execution of payment instructions.

The PSU is obliged to use a payment instrument in accordance with the terms governing the issuing and use of the instrument, and in particular, the PSU has to notify the PSP or the entity specified by the PSP, without undue delay on becoming aware of loss, theft or misappropriation of the payment instrument or of its unauthorized use. The PSU shall, as soon as he/she receives a payment instrument, take all reasonable steps to keep its personalized security features safe (Article 56(1) and (2); and see also Article 58).

The PSP has to meet the obligation of having to ensure that the personalized security features of a payment instrument are not accessible to parties other than the holder of the payment instrument (without prejudice to the obligations of the PSU mentioned above). The PSP further has to refrain from sending an unsolicited payment instrument, except if such payment instrument held by the PSU is to be replaced. The PSP also has to ensure that appropriate means are available at all times to enable the PSU to notify the PSP of any loss, theft or misappropriation of the payment instrument or its unauthorized use. This includes an obligation on the PSP to provide the PSU with the means to prove, for 18 months after notification, that he/she has made such notification. Finally, the PSP must prevent all use of the payment instrument once notification has been made (see Article 57(1)). The PSP bears the risk of sending a payment instrument to the payer or of sending any personalized security features of it (Article 57(2)).

It is further provided that member states have to require that, where a PSU denies having authorized a completed payment transaction or claims that the payment transaction was not correctly executed, the PSP bears the onus of proving that the payment transaction was authenticated, accurately recorded, entered in the account and not affected by a technical breakdown or some other deficiency. The use of a payment instrument recorded by the PSP would not, *per se*, be sufficient to establish either that the payment was authorized by the PSU or that the PSU acted fraudulently or with gross negligence (Article 59).

The Directive also provides for the liability of both the PSU and PSP. member states have to ensure that, in the case of an unauthorized payment transaction the PSP refunds the PSU with the amount of the unauthorized transaction, or, where applicable, restores the payment account that had been debited with that amount to the situation that would have existed had

the unauthorized payment transaction not taken place. Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the PSP and the PSU (Article 60). However, a PSU will bear the loss up to a maximum of EUR 150 resulting from the lost or stolen payment verification instrument before he/she has notified the PSP of such lost or stolen payment verification instrument, except if the PSU acted fraudulently or with gross negligence. The amount may be further reduced by member states, provided that such reduction does not apply to PSPs authorized in other member states. Once the PSU has notified the PSP of the loss or theft of that payment instrument, the PSU will not bear any financial consequences resulting from such loss, theft or misappropriation, except if he/she had acted fraudulently or with gross negligence. If the PSU acted fraudulently or with gross negligence with regard to his/her obligations, he/she has to bear all the losses of unauthorized transactions. In such cases, the maximum amount does not apply. If the PSP does not provide adequate means for the notification at all times of a lost, stolen or misappropriated payment verification instrument, the PSU will not be liable for the financial consequences resulting from use of that payment verification instrument, except where the PSU has acted fraudulently (Article 61).

The Directive makes provision for refunds of payment transactions initiated by or through a payee which have already been executed if the authorization did not specify the exact amount of the payment transaction when the authorization was made and the amount of the payment transaction exceeded the amount the payer could reasonably have expected, taking into account his/her previous spending pattern the conditions of his/her framework contracts and relevant circumstances of the case (for more detail see Article 62). Member states must ensure that the payer can request the refund referred to above. Within 10 days of receiving a request for a refund, a PSP must either refund the full amount of the payment transaction or provide justification for refusing the refund, indicating the bodies to which the payer may refer the matter (Article 63).

It is evident from the above that the Directive has harmonized the principles of unauthorized payments within the European Union and that the obligations of PSUs and PSPs are clearly spelled out.

4 South Africa

4 1 Internet payments and standard agreements

In South Africa, all the more recent payment instruments, such as payment cards, EFTs and internet payments, are governed by agreement between the bank as issuer and its customer. In most agreements the banks as card issuers limit their liability in the event of malfunctioning of their electronic fund transfer unit (EFT Unit) resulting from circumstances beyond the reasonable control of the bank or for any losses suffered by the cardholder

as a result of the unauthorized access to any data. The same applies in the event of incorrect information being supplied through an EFT Unit. Where the EFT Unit is used in conjunction with a card, the cardholder is liable for any losses incurred up to the time of notification of the loss or theft of such card, as in the case of credit cards. An examination of a few of the local standard contracts concluded by banks with customers to effect third party payment via the internet, reveals that the banks have ensured that the greatest extent of liability is borne by the customer (see Lawack-Davids *Internet Instruments* 243 for examples of local standard contracts). In terms of some agreements the customer waives any claim which he/she may have or acquire against the bank and indemnifies the bank against any claim by any third party. The customer will be responsible for any loss suffered or incurred by him arising from the customer or nominee making use of the service, unless such loss arises due to the bank's wilful misconduct or gross negligence. Apart from this type of clause, it is mostly stated that should the client or nominee make an error in payment, the bank shall endeavour to assist in correcting the error(s), but will not be liable for any loss resulting from such error. The bank is also not liable for the failure or unavailability of the system. In addition, in terms of some agreements the customer undertakes that the bank shall not be obliged to verify the destination account numbers, parties' names or the amounts involved in any instruction and, in the event of a discrepancy in such a payment instruction between the destination account number and the name of the party concerned, the destination account number shall prevail.

Benner ("Commercial Law: Loss Allocation under U.C.C. Article 4A" 1990 *Annual Survey of American Law* 239 243) argues that funds transfers have a two characteristics that distinguish them from other types of electronic payment instruments, and that these characteristics explain why banks are eager to avoid liability for loss of funds or other damages. These two characteristics are firstly, that electronic funds transfers involve payments of large sums of money among highly sophisticated business and financial institutions. The second characteristic is that these transfers are quick, very inexpensive to perform and that their cost has no relation to their size.

The cost of a funds transfer is derived entirely from the mechanical operation involved in the transfer. If banks are going to be liable for potentially enormous losses, then they will charge more for these transactions and perhaps cause more customers to use the time-consuming process of cheque collection (Benner 1990 *Annual Survey of American Law* 243-244).

4 2 Possible changes in the common law in light of Barkhuizen v Napier (2007 5 SA 323 (CC))

The above was the position until the seminal judgment of the Constitutional Court in *Barkhuizen v Napier.* In this decision the Constitutional Court had to deal, *inter alia*, with the question whether a limitation clause in an insurance

contract could be avoided on the grounds that it was inconsistent with public policy. A number of interesting and very relevant principles relating to the maxim *pacta sunt servanda*, the role of the Constitution in developing the law of contract and especially the notion of public policy were discussed.

The court decided that the principle of *pacta sunt servanda* is subject to constitutional control (330G).

> "I do not understand the Supreme Court of Appeal as suggesting that the principle of contract *pacta sunt servanda* is a sacred cow that should trump all other considerations. That it did not is apparent from the judgment. The Supreme Court of Appeal accepted that the constitutional values of equality and dignity may, however, prove to be decisive when the issue of the parties' relative bargaining positions is an issue. All law, including the common law of contract, is now subject to constitutional control. The validity of all law depends on their consistency with the provisions of the Constitution and the values that underlie our Constitution. The application of the principle *pacta sunt servanda* is, therefore, subject to constitutional control."

This decision was considered and applied in several subsequent cases (see amongst others *De Braven (SA) (Pty) Ltd v Byrne* 2008 6 SA 229; *Advtech Recoursing (Pty) Ltd t/a Communicate Personnel Group* 2008 2 SA 375 (C); and *Bredenkamp v Standard Bank of South Africa* (2010 4 SA 468 (SCA)). In *Bredenkamp*, the Supreme Court of Appeal made it clear that a court will not readily interfere with the enforcement of a contractual term simply because it is unfair. Interference will only be warranted if a term or its enforcement is contrary to accepted constitutional values (par 46-50).

It is submitted that many clauses in contracts between issuer banks and their card customers may fall foul of the test in *Barkhuizen* and that the customer may be afforded more protection than before. This will be especially true where banks deal with customers who have much less bargaining power than the bank (see *Barkhuizen* 341G).

The position regarding unfair or unreasonable terms in contracts will, in future, be regulated by sections 48 to 52 of the Consumer Protection Act 68 of 2008 (see par 4 4 below).

4 3 The Electronic Communications and Transactions Act ("ECT Act")

The ECT Act (Act 25 of 2002) contains some consumer protection measures in Chapter VII of the Act. This Chapter is closely aligned to the European Directive on Distance Selling (see Lawack-Davids *Internet Instruments* 123, for a more detailed discussion of this Directive).

A consumer is defined in the Act as any natural person who enters or intends entering into an electronic transaction with a supplier as the end-user of the goods or services offered by that supplier (see s 1). It is important to note that the consumer protection provisions apply to electronic transactions only (see s 42(1)), but the provision relating to the cooling-off period does not apply to certain electronic transactions. One of the important

exclusions is that of electronic transactions for financial services, including, but not limited to, investment services, insurance and re-insurance operations, banking services and operations relating to dealings in securities (s 42(2)). It is submitted that it is erroneous to argue that electronic transactions for financial services are excluded from *all* the consumer protection measures in the Act (authors' own emphasis). It is evident that the exclusion of financial services is only with regard to the cooling-off period in section 44 and that the other provisions do apply to such transactions. Chapter VII also does not apply to regulatory authorities established in terms of a law if that law prescribes consumer protection provisions in respect of electronic transactions (s 42(3)).

A website owner who offers goods or services for sale, for hire or for exchange by way of an electronic transaction, has to bear in mind that the Act lists 18 pieces of information, which must be made available to consumers on the website. This list is extremely helpful with regard to the type of information that must be made available to consumers on a website. However, it does not cover the content of some of the procedures and policies. For example, it provides that the security procedures and privacy policy of that supplier in respect of payment, payment information and personal information must be made available, but it does not describe or give guidelines on what such security procedures and privacy policy should entail.

In addition to this information, the supplier must provide a consumer with an opportunity to review the entire electronic transaction, to correct mistakes and to withdraw from the transaction, before finally placing any order (s 43(2)). Failure to make the information listed above available to consumers and to provide the opportunity for revision, entitles the consumer to cancel the transaction within 14 days of receiving the goods or services under the transaction. If a transaction is so cancelled, the consumer has to return the performance of the supplier or, where applicable, cease using the services under the transaction. In addition, the supplier has to refund all payments made by the supplier, minus direct cost of returning the goods.

The supplier must execute the order within 30 days after the day on which the supplier received the order, unless the parties have agreed otherwise. Failure to do so entitles the consumer to cancel the agreement with 7 days' written notice. If a supplier is unable to perform in terms of the agreement on the grounds that the goods or services are unavailable, the supplier must immediately notify the consumer of this fact and refund any payments within 30 days after the date of the notification (s 46).

It has to be noted that the protection afforded to consumers applies irrespective of the legal system applicable to the agreement in question. This means that if a consumer buys a book at Amazon.com, he/she will still have the protection of Chapter VII of the Act. Furthermore, any provision in an agreement which excludes any rights provided for in this Chapter is null and void. The parties can therefore not state that, for example, English law is applicable to their agreement and attempt to exclude the consumer

protection provisions in the ECT Act. Time will tell whether this will indeed be acceptable to overseas companies. Finally, a consumer may lodge a complaint with the Consumer Affairs Committee in respect of any non-compliance with the provisions of Chapter VII by a supplier (ss 47-49).

From a payments perspective, it is important to note that the Act provides that the supplier must utilize a payment system that is sufficiently secure with reference to accepted technological standards at the time of the transaction and the type of transaction concerned. The supplier is liable for any damages a customer suffers as a result of the failure by the supplier to comply with this requirement (s 43(4) and (5)). Unfortunately, the Act does not give guidance on the meaning of "sufficiently secure". It is also not certain what the accepted technological standards would entail. It is understandable that technological neutrality was probably at the back of the minds of the drafters. However, it makes it very difficult for website owners to be sure that the security system that they use for their payment systems is indeed "sufficiently secure" with reference to accepted technological standards prevailing at the time. It is, therefore, important that someone must determine these standards from time to time. It is not clear whether this needs to be determined by the stakeholders in the National Payment System (NPS) or whether it can be left to the information technology (IT) industry. Website owners must, therefore, keep abreast of the latest security solutions employed with regard to payment systems and payment instruments. This may have some cost implications which will have to be borne in mind by website owners.

4 4 The Consumer Protection Act (CPA)

The Consumer Protection Act 68 of 2008 will come into operation on 1 April 2011. The Act provides for sweeping changes in consumer protection law in South Africa. The Act will drastically change the way in which South Africans conclude contracts in all walks of life, including contracts and payments over the internet. In general, the Act contains more encompassing protection than chapter seven of the ECT Act. The legislator has, in an attempt to synchronize the two acts, excluded the working of the CPA in certain cases where the consumer protection provisions of the ECT Act have made provision for protection. Some of these exclusions benefit the electronic consumer while others place the consumer in a weaker position than other consumers.

The CPA contains the following provisions which refer directly to electronic transactions: Firstly, it recognizes electronic as well as advanced electronic signatures (s 2(3)). It is submitted that this section is of no consequence because of the clear provisions of section 13 of the ECT Act which provide under which circumstances electronic signatures will be recognized. It further provides (s 2(4)) that a supplier must take reasonable measures to prevent the use of a consumer's electronic signature for a purpose other than the endorsing of the particular document that the consumer intended to sign. With regard to the cooling-off period, the CPA

provides that it does not apply to a transaction if the cooling-off period of the ECT Act is applicable (s 16 of the CPA). In this instance the ECT Act gives longer protection (seven days as opposed to the five days provided for in the CPA in cases of direct marketing). The provisions of the CPA further do not apply if the performance of the contract is governed by section 46 of the ECT Act (s 19(1)(b) of the CPA). Section 46 provides that performance must take place within 30 days unless otherwise agreed while the CPA provides that performance must take place within a reasonable time unless otherwise agreed (s 19(2)). It is submitted that the consumer in terms of the ECT Act will normally be in a better position because there will be no need to prove that a "reasonable time" has elapsed as in the case of the CPA. There are, however, provisions of the CPA which are not applicable to electronic transactions and which can be detrimental to the consumer. Most notable in this regard is the passing of the risk of delivered goods. Section 19(1)(c) provides that, unless otherwise agreed, the risk remains with the supplier of goods until delivery. There is no reason why the electronic consumer should be excluded from this provision.

The provision of the CPA with regard to the keeping of sales record (s 26) does not apply in cases where section 43 (provision of certain information to consumer) of the ECT Act is applicable. It is submitted that section 43 of the ECT Act provides sufficient protection to consumers in the electronic environment. Section 33 of the CPA relates to catalogue marketing and also does not apply if the consumer protection provisions of the ECT Act (Chapter 7) are applicable. It is submitted that this is a sweeping exclusion and can be detrimental to the consumer in the electronic environment. Finally, the CPA amends the ECT Act by replacing references in the ECT Act to the "Consumers Affairs Commission" to the commission established in terms of the CPA (schedule 1B of the CPA). This is simply an alignment of the ECT Act to the CPA regarding the body to which complaints can be made.

It is submitted that the above-mentioned exclusions are only relevant where one has to do with natural persons since the consumer protection provisions of the ECT Act are only applicable to natural persons. The exclusions are, therefore, not applicable to juristic persons.

From a payment perspective, one may mention that the term "service" in the CPA is defined to include "any banking services, or related or similar financial services … except to the extent that any such service – (i) constitutes advice or intermediary services that are subject to regulation in terms of the *Financial Advisory and Intermediary Services Act*, 2002; …" (s 1). It is submitted that banking services such as the provision of credit cards as well as services such as internet banking services fall within the ambit of the Act. This would mean that a consumer can avail himself/herself to the CPA and, most notably, to section 48 which provide that a supplier of goods or services may not make use of unfair, unreasonable or unjust contract terms.

4 5 Analysis

Although the ECT Act as well as the Consumer Protection Act provide protection to consumers in many areas, it is submitted that the issue of protection of consumers who suffered loss as a result of erroneous payments or unauthorized payments is not adequately addressed in South African law. In this regard, the situation is entirely different from that in the European Union and as discussed earlier. It is a pity that the ECT Act or CPA does not have a similar provision to Article 8 of the EU Distance Selling Directive which deals with fraudulent card payment in distance selling contracts such as internet agreements. It is evident that specific legislation is needed in the form of a Payments Act, which can focus on payments-related issues, as opposed to the payment *system* issues dealt with in the National Payment System Act (authors' own emphasis) (Act 78 of 1998 as amended by Act 22 of 2004).

Although the CPA does provide for protection of consumers in the electronic environment, it is regrettable that better synchronization between the consumer protection provisions of the ECT Act and the CPA is lacking. The CPA envisages a greater role to be played by government and consumer organizations and the Act has in this sense taken a leaf out of the books of countries such as the United States and countries in the European Union. In particular, the CPA envisages a role for "accredited consumer bodies". It is unsure at this juncture whether the role to be played by consumer bodies in terms of the CPA will extend to the payments environment.

It is submitted that compliance with the requirements of the ECT Act will go some way towards minimizing the risks outlined above. However, due to the remaining uncertainties, it is submitted that compliance with the Act needs to be complemented by mechanisms which would to a great extent ensure that neither organizations, nor their clients are detrimentally affected. Preventative measures are therefore all the more important. These could include the following: encryption, firewalls, intrusion detection systems, incident response guidelines, monitoring, external audits and authorized hacking.

5 Conclusion

Notwithstanding the inroads made by the ECT Act, the CPA and the *Barkhuizen* case, it is clear that legislation aimed at, *inter alia*, protecting internet consumers who make use of payment instruments is needed. It is evident that consumers who make payments over the internet are less protected than consumers who use payment instruments governed by legislation, such as bills of exchange and cheques. It is submitted that a more equitable loss-allocation structure can be achieved in South Africa by implementing legislation which imposes a tier structure of liability, such as in the European Union as explained above, which clearly stipulates the rights

and obligations of holders (users) and issuers of payment instruments. To ignore this challenge would only compound the problems highlighted above. In the meantime, a customer has to use preventative security measures to ensure that he/she will not be found out of pocket due to unauthorized, fraudulent or erroneous payments over the internet. At the end of the day, in the absence of adequate legal protection, a consumer has to take a calculated risk in respect of his/her choice of payment instrument. Further, and especially in the light of the CPA, the need for consumer education cannot be over-emphasized.

Vivienne A Lawack-Davids
and
Frans E Marx
Nelson Mandela Metropolitan University, Port Elizabeth