International Journal of Business, Human and Social Sciences
ISSN: 2517-9411
Vol:5, No:5, 2011

Electronic Commerce: Costumer Protection In Electronic Payments

Omid Ghassemi

***Abstract*—**As a by-product of its "cyberspace" status, electronic commerce is global, encompassing a whole range of B2C relationships which need to be approached with solutions provided at a local level while remaining viable when applied to global issues. Today, the European Union seems to be endowed with a reliable legal framework for consumer protection. A question which remains, however, is enforcement of this protection. This is probably a matter of time and awareness from both parties in the B2C relationship. Business should realize that enhancing trust in the minds of consumers is more than a question of technology; it is a question of best practice. Best practice starts with the online service of high street banks as well as with the existence of a secure, user-friendly and cost-effective payment system. It also includes the respect of privacy and the use of smart cards as well as enhancing privacy technologies and fair information practice. In sum, only by offering this guarantee of privacy and security will the consumer be assured that, in cyberspace, his/her interests will be protected in the same manner as in a traditional commercial environment.

***Keywords*—**Consumer, Electronic, Jurisdiction, Payment

I. Introduction

THE advent of a booming industry transposed to digital *loci*, commonly referred to as electronic commerce, monetary exchange has received somewhat of a persistent attention. As the digital age becomes more and more part of our every day life, and businesses are rushing to pile into e-commerce, the notion or concept of money has to be revisited in order for it to be aligned with the present commercial mandates. In Glyn Davies' "A History of Money", the author lists six specific functions of cash in hand- from units of account to stores of value; not one of them depending on the moulding of coins or the printing of notes[1]. Such an observation has become even more pragmatic within the context of electronic commerce. Yet, transposing money from the mere exchange of clinging coins to less visible to the layman forms of consideration has been a concept not new. The presence of new forms of monetary exchanges in the form of substituted contractual debt transfer from one to another has been well established in exchanges where locality and practicality so demand. Presently, the definition of money or electronic money used or desired to be used in electronic commerce transactions has been the subject of much debate[2], yet reaching a consensus on the exact scope of the definition when viewed in the light of the problems posed by electronic commerce has been far from easy. Brussels [3] has recently provided a definition to electronic money, such being characterized as 'an electronic surrogate for coins and bank notes'. One would thus be right to assume, that: *"its purpose is not therefore to simply act as another means of payment but instead to provide an alternative to payment by cash."*[4] Yet dwelling into a legalistic approach in grasping the evolution of tangible money to digital money may prove to be elusive when viewed in the light of the recent changes that technology has brought in field of electronic payments. Whilst however, the challenges may be many, especially in the field of consumer protection, considering the legal implications of digital *expender* [5] without taking a brief glance on the way electronic commerce has heralded the revision of payments may prove misleading.

Omid Ghassemi , Department of Law, Science and Research Branch, Islamic Azad University, Khouzestan, Iran.

II. The Problems Posted

It has been grossly emphasized that: *'the existence of suitable payment systems is critical to the development of electronic commerce'*. [6] Such an observation should not be overlooked. Given the ever expanding applicability platform that electronic commerce provides to innovative business ideas, one would take for granted that at least the people that would wish to interact with the digital divide should be able to: *'take some spending money when they go there.'*[7] Yet, it would be false to assume that the current payment mechanisms, such as credit and debit cards, as such have been used increasingly over the years, especially with regards to commercial exchanges over the telephone and/ or fax, have no place in the cyberspace commercial arena. It is submitted that such payment mechanisms have managed to encompass most of the needs that modern commercial transactions demand, yet they have however fallen short in balancing the needs of a business wishing to replicate its business model in the context of e-commerce alongside the need for replication of payment elements within those operations [8]. Electronic commerce has posed serious challenges to what used to be known as sales and commercial activity over a distance. It has been increasingly pertinent to the actors of the electronic divide to urge for the creation of mechanisms whereby cash can be used in the same way as normal non-electronic transactions.

Most commercial services active on the Internet have adjusted their return strategies to the models provided by conventional payments cards such as credit, debit or charge cards [9]. Yet, such conventional payment mechanisms have proven to hamper the innovative stimulus that electronic commerce provides to new entrepreneurs. To this, one can attribute the relatively costly nature of processing and collecting payments. Thus, whilst the applicability of credit cards for example may sometimes prove to be practical for relatively large payments, other purchases of a lesser value may find no way of being collected or processed by the established credit transferring payment schemes. Furthermore, card payments cannot be effected between consumers, such payments being limited to b2c relationships [10]. Given that the Internet provides modes of exchange through various

channels of modern entrepreneurship, such avenues of fiscal exchange are hampered. To this, the ever- increasing popularity of online auctions, eBay or Ubid, being such examples, has surfaced the need for: *'systems which allow for the transfer of value between consumers, rather than only between consumers and businesses.'*[11]Additionally, publishing houses, newspapers and magazines have found it increasingly difficult to transpose their commercial enterprises over the internet given the intricacies that surround the current conventional payment instruments with regards to micro-payments, most of them resorting as a result, to the somewhat less attractive subscription business model. Given the expedience and practicality the internet provides for obtaining materials, such as pictures, articles, music, software, payment schemes such as the present ones have hampered the medium's efficacy. Furthermore, the unavailability of credit cards to a considerable proportion of the population such as children and individuals having bad credit or low income have also contributed to the creation of disincentives for modern or innovative commercial models.From a consumer protection standpoint, conventional payment schemes have also given rise to various problems concerning fraud, credit card detail interception in addition to those relating to fears emanating from the financial stability of the issuer which have played a role in preventing the use of such mechanism from being fully exploited by the market within the context of electronic commerce.

III. Technology At The Forefront

A. Tightening the Grip of Conventional Payment Cards

From a consumer protection standpoint, the risks pertaining to the use of credit or debit cards for sales over the Internet has somewhat mandated the revision of the already existing credit transfer protocols. Fears associated with credit card detail interception over the Internet coupled by the anonymity haven that the Internet provides to unscrupulous merchants have done much in hampering consumer confidence. To this, the popularity that the existing payment cards have gained over the years, even before the development of electronic commerce along with the success of the card companies in managing to have their product effectively sunk in to common commercial practices have somehow played a deterrent role in simply discarding their use altogether. Instead, technology has yet again joined the digital playing field in order to develop and re-adjust the card payment schemes in a way that confidence can be regained and use of such systems can go on uninhibited. Whether the said plans have been achieved, has to be viewed in the light of the legal framework surrounding electronic payments, a subject dealt with later on in this study.

The capabilities provided by encryption have once again, aided in securing the transmission of individual card details over the Internet. In 1998, Netscape patented the SSL protocol [12] and submitted it to the World Wide Web Consortium as a standard, such protocol: *"creating a secure channel for the transmission of encrypted payment card details between retailer and consumer."*[13] By the use of public and private key encryption, SSL has been used effectively in transmitting card payment details effectively and safely over the Internet, becoming in this way the *"norm for secure communication of payment."*[14]Card details are submitted and encrypted, thus transmission is safeguarded against interception since the information can only be deciphered by using the respective private or public keys that are within the possession of the relevant parties to the transaction. Risks inherent in the interception of card details are thus significantly reduced while fears pertaining to the intentions of the respective parties remain intact as the protocol has done nothing to reduce the anonymity factor, underlying most fraud cases since both the consumer and the e-tailer have no true knowledge of each other.The above issues, unfortunately being abound in internet transactions and that were not dealt with by the SSL protocol were the subject of the combined work conducted by Netscape, MasterCard and Visa in coming up with the SET standard.[15] The SET standard has targeted the problems and risks pertaining to anonymity as, by the use of sophisticated encryption mechanisms similar to the ones found in the SSL protocol, has managed to leave the issue of certification on Banks who are the only ones that may decipher and further transmit card details once the identities of the respective parties has been carefully ascertained. Public and private key encryption are again used coupled by the requirement that the respective parties must be registered with the SET standard along with certification authorities that will authenticate the parties, features in the standard that some commentators have noted as acting as a disincentive to its popularity[16].Fears emanating from the need of limiting the anonymity factor present in Internet transactions have inspired the use of various systems whereby payments are effected through means other than sending card payment details directly to the retailer. Thus, in cases where consumers may find themselves uneasy in transmitting their details directly to merchants, alternatives exist whereby their details can be stored on the servers of third party companies such as Cyber Cash or companies that can process credit card details such as Netbank Ltd. Users using such services can send their details to these companies after such details have been encrypted using the software provided by them. Where a transaction needs to be effected contact is established with the retailer in the form of a validated invoice for example, the latter having no means of accessing the details and the processing then takes place through the Banks who will have been instructed by these intermediaries[17]. Whilst these sort of schemes do enough to promote trust with regards to authenticity of the respective parties to a transaction, they fail however to address issues relating to the solvency and financial stability of the said intermediaries.Risks relating to credit card detail interception have been addressed by merchants themselves by creating databases whereby card details are stored by the consumer only once, such details then being kept at the server of the proprietor and retrieved by the consumer upon his next purchase from the merchant. Examples of such methods can be seen extensively throughout the Internet, mostly at sites of online booksellers such as Amazon and Barnes & Noble. Fears relating to the identification of the card-holder can be eliminated, at least in regards to potential liability from the merchant by the use of a password by the consumer who will gain access to the details of the card upon his/ her next visit to the merchant's website. Whilst these methods address the

issue of risk of credit card detail interception for frequent buyers who will have to re-submit their details on every visit, one would be wrong to assume that these systems are immune from hackers using sophisticated technology.

B. Alternative Methods to Conventional Payment: Cards Expired Yet?

The problems that surround the use of traditional payment mechanisms have been gradually brought to the surface with reference to transactions conducted over the internet. Issues relating to security, anonymity, fraud etc. that were briefly noted above have been the subject of research and practice by many institutions yet the costly nature of the system, the system's inapplicability to all the sectors of the population in addition to its inadequacy for minimal payments (or micro-payments) have heralded the need for change. The advent of the use of smart cards by various industry sectors has exposed the said mediums' efficacy in regard to payments as well, be they over the Internet or even in the 'real' world. Whilst the conventional card payment market has been allegorized as a *"tree dominating a garden"*[18] the innovation of different payment mechanisms either based on smart card technology or on software but both aiming at addressing problems posed by conventional card schemes has proven to be a targeted aim by all players of the electronic commerce arena. One of the main advantages of the already developing system is that payment can be effected on an on-the-spot basis, thus departing from the credit relationship that credit cards for example provide whereby the consumer transfers the obligation to pay a merchant to the card issuing company or bank as the case may be. It is aimed that transfer of funds is to take place instantaneously through means that encourage the creation of accounts even of limited funds, harboring thus sectors of the population such as children or low-income individuals that are already great participants of the Internet. [19]The popularity that smart cards have been gaining for payment mechanisms for payments both online and offline has been realized by the creation of various schemes whereby users can use cards which are equipped with smart cards for payments. Such payments can be made both from consumer to businesses as well as between consumers [20]; business-to-business exchanges not being covered by the scheme. Smart card based schemes, which would include systems such as Mondex, Visa Cash and Proton are quite practical in their use since they can be loaded with cash [21], some up to a certain amount, from an ATM and then used on the premises of a shop by inserting the card on the hardware provided, whereby the user inserts his/her Personal Identification Number authorizing the transfer of funds. Encryption is used for increased security, keys being used by the Bank and the consumer [22], the former authenticating the transaction. In addition, such schemes provide the opportunity for use of such cards on transactions carried out on the Internet by the provision of software and hardware that can be downloaded and connected onto the user's terminal. Such systems however are limited to those that willfully participate in the schemes. From a legal standpoint, the regulatory regime that governs such institutions is far from being clear, thus hampering the protection afforded to consumers that use such payment mechanisms [23].Additional payment schemes have been developed that operate on a similar level to the ones based on smart card technology mentioned above but using software installed on the user's computer and all transactions carried on from there, having no tangible card or bank account. It could be said that such payment systems have been developed specifically for payments on the Internet so factors such as practicality and efficacy have been grossly considered by the institutions that have launched such systems. Systems such as these, examples of which would include e-Cash and Barclay Coin, operate on the basis of the consumer approaching a financial institution such as a bank that runs or participate in such a scheme and open electronic cash account [24]. The consumer or merchant is provided with software whereby a purse or an account is created and all transactions are carried out from there. Upon transfer of funds from the real account to the electronic one, cash is 'transformed' in to units or tokes or electronic coins that the holder can use for his/her purchases. Each coin or token is given a serial number by the financial institution and upon its use; the serial number is recorded thus avoiding the case of multiple use. Anonymity is also safeguarded through this system. In addition to the problems posed by regulation in terms of defining the operation of these institutions thus finding it difficult to pigeon hole the regulatory regime the institution falls under, problems of definition also arise since it is questionable as to whether these tokens or coins can fall under the definition of money provided by the Electronic Money Directive [25].

IV. The Legal Framework Of Electronic Payment Instruments

One of the most pertinent risks in the online marketplace that inhibits consumers' confidence in electronic commerce is the risk of financial loss due to fraudulent credit card transactions. A legal response to these legitimate concerns whether there would be any protection for the consumer in cases they suffers loss, is given to an extent by the consumer credit laws of the countries in which the card is issued. One example is the UK Consumer Credit Act 1974 which provides that a credit card holder is not liable to his bank (card issuer) for 'any loss' arising as a result of the unauthorized use of the card.[26] Such a provision however is subject to s.84 (1) according to which cardholders can be held liable for the first 50 pounds in case of loss, provided the credit card was misused while out of their possession.[27] In cases of fraudulent online transactions by credit cards the issuing banks usually suffer no loss since in these circumstances 'charge-back' clauses effectively place the risk of such fraudulent transactions upon the merchant.[28] In cases where the consumer purchases e-goods using his credit card but receives no goods or defective goods, the Act provides that the card issuer is jointly liable with the supplier for breaches of contract and tort.[29]

A. Directive on Unfair Terms in Consumer Contracts:

Generally, the contractual relationship between the issuer and the consumer is governed by the issuer who is in a stronger bargaining position and offers the contract on a 'you like it, you take, you don't like it, you leave it' basis.[30] The Directive on Unfair Terms in Consumer Contracts was

designed to protect the consumer from being bound by unfair terms.[31] Unfair is defined any contractual term 'which has not been individually negotiated and contrary to the requirements of good faith causes a significant imbalance in the parties' rights and obligations under the contract, to the detriment of the consumer'.[32] , Article 7 of the Directive provides that Member States shall ensure that 'adequate and effective means exist to prevent the continued use of unfair terms in contracts concluded with consumers by sellers or suppliers'.[33]

B. Recommendation 97/489/EC of 30 July 1997

In 1997 the European Commission issued its Recommendation, which concern transactions made by electronic payment instruments and govern the relationship between the card issuer and the cardholder, by establishing the obligations and liabilities of both parties in cases of unauthorized use of the electronic payment instrument due to loss, theft or falsification of the system.[34] The issuer in a 'good time prior to the delivering an electronic payment instrument' is under the obligation to communicate to the holder the contractual terms and conditions governing the issue and use of the payment instrument. The terms of the contract must include the issuers' obligation not to disclose personal identification numbers or other codes to anyone except from the legitimate cardholder.[35] If the issuer violates these obligations he is liable for any payments made by persons other than the cardholder. Furthermore, the issuer must provide the consumer with all the appropriate means so as to enable the holder to make the notification required by the Recommendations in the event of loss, theft or error.[36] Upon notification of the loss, fraud or error of the payment instrument, it is legally incumbent upon the issuer to place a block on all technical devices, in order to stop any further fraudulent use of the payment instrument.[37] Failure to do so means that the issuer is not entitled to charge the cardholder for any payments made after receipt of notification of the card's loss or theft. [38]Additionally, the issuer is liable to the holder of an electronic money instrument for the lost amount of value stored on the instrument and for the defective execution of the holder's transactions, 'where the loss or defective execution is attributable to a malfunction of the instrument, of the device/terminal or any other equipment authorized for use, provided that the malfunction was not caused by the holder knowingly or in breach of Article 3(3)(a).[39] On the other hand is essential for the cardholder to take all the necessary steps to ensure the safety of the payment instrument and of all the means, which enable it to be used (PIN).[40] The other main obligation of the cardholder which is essential when determining liability, is to notify to the issuer (or the entity specified by the latter) without delay the loss or theft of the electronic payment instrument or of the means which enable it to be used, the recording on his/her account of any unauthorized transaction, or any error or other irregularity in the maintaining of that account by the issuer.[41]In establishing liability the exact moment of notification is of crucial importance. Up until notification the consumer bears responsibility for the sustained losses due to the loss, theft or fraudulent use of the payment instrument up to a limit of 150 EURO. [42] After notification the liability is transferred from the holder to the issuer.In cases where it is proved that the consumer has acted with extreme negligence or fraudulently the issuer bares no responsibility for the losses sustained.[43] It is the cardholder who has to establish that the transaction was unauthorized.[44] However, as explained above, if the discovery of the identification number for example and the subsequent unauthorized use of the payment instrument occurs after notice has been given to the issuer, then liability under the Recommendation is transferred to the issuer.

C. E-money Directive

One of the main risks for e-consumers when they use electronic money is the financial loss due to the originator's (issuer) insolvency or withdrawal from the scheme. A legal response to these legitimate concerns was given by the so - called E-Money Directive [45]The major objective of the Directive is to set up a prudential legal framework aiming at safeguarding the financial integrity and stability of E-money institutions as well as ensuring their supervision, issues that are of vital importance in establishing consumers' confidence in electronic payments and e-commerce. The Directive provides that the bearer may ask the issuer to redeem the electronic money at par value or by a transfer to an account free of charge other than those necessary to carry out the transaction. Furthermore, in order to minimize the risks of the originator going insolvent and therefore of the consumer suffering financial loss, the E-Money Directive lays down clear capital and on-going funds requirements.[46] Thus under the Directive the initial capital of an electronic money institution should not be less than 1 million EURO whereas the institutions own funds should not be less than 2% of the higher of the current amount or the average of the six proceedings months total amount of their financial liabilities.[47] The purpose of such provisions is to ensure in cases of loss in the invested money, the issuer will have sufficient funds to act as 'cushion' so as to redeem money that consumers may possess and also to pay retailers who have already received electronic money.[48] For the same reasons, the Directive also imposes limitations on the types of investments in which money can be placed.[49]

D. Proposed Directive on distance marketing of consumer financial services [50]

The Directive establishes the necessary legal framework with respect to new techniques used for the distance marketing of financial services.[51] In relation to financial loss that might incur due to fraudulent and unauthorized use of the electronic payment instrument, Article 8, provides that Member States shall take appropriate measures to ensure that a) consumers can request cancellation of a payment in the case of fraudulent use of their payment card in transactions falling within this Directive and b) in the case of fraudulent use, the amounts paid are reaccredited or that the consumer is reimbursed.[52]

E. Distance Selling Directive [53]

Article 8 provides that 'Member states shall ensure that appropriate measures exist to allow a consumer a) to request cancellation of a payment where fraudulent use has been made

of his payment card in connection with distance contracts covered by this Directive; b) in the event of fraudulent use, to be reaccredited with the sums paid or have them returned. The consumer can only be held liable if his negligent conduct caused the misuse. However, the transmission of credit card details over the Internet, even over insecure channels, cannot be deemed to constitute negligent behavior on the cardholder's behalf.[54] 5. To what extent are consumers protected under the current legal framework? In a study that was completed in May 2001, the researchers identified a number of problems in relation consumer protection with respect to electronic payment instruments. The following were pointed out: [55]

1. The Recommendation's aim to create transparency of conditions for transactions is not achieved in four main respects. [56]

2. There is a substantial level of non-compliance with the Recommendation in relation to the obligations and liabilities of the parties to the contract.

3. Many issuers do not comply with the Recommendation in respect to the procedure for notification for loss or theft and the issuer's liability after notification.

4. In most Member States the burden of proof is placed on the holder or at least not stated in the EPI contract terms.

5. The means for dispute settlements are inadequate.

E-money Directive on the other hand brought to a great extent the desired result. It put an end to the ongoing dichotomy between the financial and non-financial, in as far as their supervision is concerned Provisions of redeem-ability, capital requirements and investments restrictions should be credited as moving a step ahead in enhancing consumer confidence in e-payments and therefore in e-commerce. There are however, some grey areas such as paragraph iv of the definition which poses questions as to which organizations fall within the Directive's provisions.[57] Nevertheless, at this stage in order to judge its impact on consumers' protection we should wait and see how Member States will implement its provisions and of course how the e-payment market will develop.

V. A Step Forward

A. Stronger consumer protection legislation?

Enhanced consumer protection legislation would on the one hand foster consumers' confidence in e- commerce, on the other hand however, it might lead to a 'knee-jerk' legislative reaction that would probably inhibit the growth of new technologies and hamper further developments. The reverse may be true as well. Lax consumer protection legislation may have the advantage of encouraging e- payment systems' innovation allowing thus the market to develop, however, insufficient consumer protection legislation would inhibit consumers' confidence in new e-payment systems prohibiting thus this new market from reaching a critical mass of acceptance hampering thus the development of e-commerce.[58] Therefore, before leaping to the conclusion that new and stronger consumer protection legislation is needed, some alternatives should be considered and maybe given a chance.

B. The role of education

Consumers and e-merchants should be aware of all the features and functions of the various systems as well as all the risks of financial loss involved and their legal protection in relation to such risks. Consumers need education in relation to their liability that might incur from the use of new types of electronic money so they can understand the differences between new digital payment systems and traditional payment mechanisms in order to make their choice accordingly when buying online. In addition consumers should be armed with all the essential information regarding e-money, such as issues of privacy in order to have the ability to weight the pros and cons of these new mechanisms and maturely make his choice. [59]

Finally, under more practical terms the industry could post out questionnaires specifically designed in order to measure consumers' awareness in this evolution of payment mechanisms. This will help the industry to assess and improve its products. Seminars could also be held in national and international level in relation to the above-mentioned issues. In addition, experts from the industry, the legal field researchers and consumer protection organizations could initiate an educational campaign in public (TV, radio, presses etc.)

C. The role of technology

Technology that provides cyber criminals with the methods for illicit activities in the electronic environment may itself provide the means for fighting crime from the very beginning. [60] New technical-legal methods such as encryption and electronic signatures can play a decisive role in providing the security required in the electronic payment marketplace, filling thus up some of the gaps that current legislation leaves in relation to consumer protection.Indeed a number of technological methods in relation to credit cards as payment method for on-line purchases that involve the creation of secure protocols have already been developed.[61] These protocols use public key cryptography. The most known protocols for payment systems that have been established in today's electronic commerce market are the SSL and SET protocols.Electronic signatures could provide a useful means for detecting online fraud since they protect four important functions in law namely, authentication, signification, verification and legalisation.[62] The issuer of the message encodes his message digitally using his private code and the recipient decodes it using the public code. Thus, when receiving the data, he can be certain that the message has been sent by the holder of the authorized public code, that also holds the private code used in the message sent (authenticity), that the message has not been modified during the transmission, since a change in a single bit would have meant the obtaining of an illegible message by the recipient (integrity) and that the sender of the message may not deny being the author because the message was not 'signed' with his private code that is only known by him (no rejection in origin).[63] A smart card can incorporate for example digital – signature payment authentication system. Additionally, a number of standards have been developed or are under development such as the Joint Electronic Payments Initiative (JEPI) aiming at developing standardise application programme for negotiating payment methods between web browsers and servers which is interoperable across all Internet

payment solutions. [64] Another significant interoperability initiative is the Open Trade Protocol (IOTP) and the Common Electronic Purse Specification (CEPS). [65]

D. The role of the industry

Parallel to the existing legislation, self-regulatory regimes, general codes of conduct, voluntary industry guidelines and dispute resolution programmes could play a supplementary role in enhancing consumer protection in the electronic payments marketplace.[66] However, they should be the product of negotiations with consumer's representatives, worldwide expressing the international character of the Internet banking and cyber payments along with the global need of consumers.[67] In addition, the role of 'banking ombudsman' programmes already existent in several countries with the aim to handle banking complaints should be strengthened.[68]In some multi-issuer electronic money schemes voluntary insurance or loss sharing arrangements are anticipated so, in cases of insolvency of one of the institutions, the others would jointly honor electronic money claims issued by that institution.[69] Guaranteeing schemes on the issuer behalf could also provide some degree of confidence to e-consumers. E-businesses should also provide their consumers with insurance or a contractual shield against liability as is the case for example, with Amazon.co.uk which covers 50,00 pounds of the consumer's liability provided that the unauthorized use was not the result of the latter' s fault from purchases made at Amazon using the secure server. [70]

E. The role of the governments and supervisory authorities

Governments' and supervision authorities should both pursue their policy objectives so as to ensure that the relevant legal framework provides adequate incentives for fair practices and a strong foundation for reasonable private agreements and contracts.[71] They should also ensure that existing laws and industry practices are followed, the independence of ADR, and that criminal penalties in relation to fraud and theft of electronic payment instruments are applied. They should encourage industry behavior or self-regulation aiming at addressing consumer protection issues and sanction those that do not comply with the legislation or fair practices. In addition, they should ensure a right balance between the need to combat crime in the electronic which requires transaction reporting, consumers' identification and the consumers' rights of privacy and data protection.Finally, the transparency of electronic payment products, the financial integrity of the electronic money issuers and the adaptation of the required technological measures by the e-money providers necessary for the combating of crime should also be ensured.

VI. Conclusion

The advent of the Internet has signaled the formation of the Information Society and the creation of the World Wide virtual shopping centre, within which an undutiful exciting marketing revolution has commenced. Indeed a number of 'cyber-payment' products have been developed in order to facilitate e-commerce by replacing traditional money kept in purses and wallets with their digital equivalent stored on 'e-purses' and 'virtual wallets'. Although electronic payment systems that have recently been developed present a number of advantages for all the players involved in e-commerce, the electronic payment market has not been taken-off yet in the virtual world. One of the main reasons is that the virtual environment is a place where the principles of good faith and practice as well as those of trust are not well established making thus consumers reluctant in using electronic payment mechanisms. The current legal framework applicable to electronic payment provides only to an extent protection to consumers. There are still some grey areas in the current legal regime and some gaps that leave questions regarding the protection of consumers with respect to risks involved by the use of e-payment systems.In designing an effective, appropriate and adequate regulatory framework for electronic payments we have to keep a balance between different objectives and factors such as consumer protection, financial stability as well as technological innovation and competition. First of all however, it has to be understood that the role of the legislation is to 'heal' the 'financially injured' e-consumers and not to prevent the injuries from occurring. Therefore, technology has the first role to play in enhancing consumers' confidence since it can provide the means for preventing illicit activities that result in financial loss on the consumers' behalf. Provided that technological measures to protect consumers are in place, then the combination of current legislation with self regulation as well as with solutions deriving from the industry's initiatives may be proved adequate to feel the gaps that current legislation leaves, increasing thus consumers' confidence in e-commerce. Such a combination may do the 'trick' since it can provide a flexible regulatory regime that on the one hand protects consumers whereas on the other stimulates innovation and encourages competition, necessary for the development of the e-payment market.

References

[1] Peter Preston, 'The Abolition of Hard Cash? That will do nicely. Money's symbolic power is vanishing, one stride at a time', The Guardian, Monday April 17, 2000.
[2] The G10, in their 'Report of the Working Party on Electronic Money', noted that: *'a precise definition of electronic money is difficult to provide; indeed a number of official bodies have described and categorized these products in different ways.'*, April 1997.
[3] Directive 2000/46/EC on the taking up, the pursuit and prudential supervision of the business of electronic money institutions.
[4] Laura Edgar, 'Electronic Money', in Reed, Walden and Edgar, 'Cross-Border Electronic Banking: Challenges and Opportunities', 2nd ed., LLP, 2000, at page 202.
[5] Davies notes that the etymology of the words spends and pound come from the Latin *expendere*, which means to weigh. Op. cit. supra fn. 1
[6] Trystan Tether, 'Payment Systems for E-Commerce', in *supra* FN 4 at page 167
[7] 'Electronic Money: So much for the Cashless Society', the Economist, 26 November 1994, Vol.333, No. 7891, pg 3
[8] *Supra* fn. 6. At page 167
[9] Figures suggest that such cards are used to effect payment in more than 90% of the web-based transactions, cited in *supra* fn. 6 at pg. 169.
[10] Additionally, card payments are "ill-suited" to b2b transactions. Op.cit. fn. 6 at page 176
[11] Simon Newman, Laura Edgar & Gavin Sutter, 'Electronic Payments and Smart Card Systems' in Simon Newman (Ed), 'Smart Cards', ECLIP II, IST Project 1999-12278
[12] Secure Socket Layer Protocol.
[13] *Supra* n. 11.
[14] Ibid.

[15] Secure Electronic Transaction Standard.
[16] *Supra* f. 11.
[17] *Id.*
[18] Tether, op.cit. FN 6 at page 181
[19] Ibid.
[20] Mondex being the only provider of such service.
[21] Some institutions make provision for disposable cards, similar to the mobile "pay as you go" types available from most mobile telecommunications operators.
[22] Unbeknownst to him/her since the key is stored within the smart card.
[23] Section B, *infra*.
[24] It is to be noted that the consumer and/or merchant must have a normal account with such banks or financial institutions already.
[25] Directive 2000/46/EC of the European Parliament and of the Council of 28.09.2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions.
[26] S 83(1) strictly applies only to regulated consumer credit agreements as defined in s.8 of the Act, which include agreements whereby a creditor (card issuer) provides a debtor (card holder) with credit that does not exceed 25,000 pounds. The provision of this section offers protection to e- consumers in cases their credit card details have been collected by a sham site.
[27] Such protection will generally not be applicable in cases where the consumer's credit card details have been intercepted on the Internet and subsequently used for unauthorized purchases or where the credit card details have been collected by an illegal, sham site, the reason being that the consumer is still in possession of his credit card in the online market and therefore does not follow under s.84 (1) provisions.
[28] More specifically, if the card holder within a certain time limit disputes a transaction claiming that is the result of fraud, theft or error, then if such a dispute is accepted by the card issuer, a charge- back will occur obliging the e-merchant not only to repay the disputable sums, but also subject himself to a possession fee which sometimes is more that than the sum in dispute.
[29] S.75 CCA1974. However, the issuer's (bank) liability under s.75 depends on the consumer's claim against the merchant, in other words it has first to be established according to the contract between the consumer and the merchant that the first has a claim against the latter. It is worth to be mentioned that the consumer apart from the purchase price of the goods, he can also claim any consequential loss that incurred by the merchant's breach of contract. Nevertheless, it has to be noted that s.75 can only be applied when three requirement imposed by the law are met:The purchase price of the goods is greater that 100 pounds and less that 30,000 pounds and;[29] - the credit card agreement is used to finance a particular transaction between a debtor (card holder) and a supplier (merchant0 and;[29] - the credit card purchase is made under pre-existing arrangements or in contemplation of future arrangements between the card issuer and the merchant
[30] For example, in the BT Array payment system one of the terms stated that 'the issuer may change the terms and conditions contained in this agreement at any time. You are advised to check the terms and conditions when using the Service to be aware of any such changes which you will be deemed to have accepted by your ongoing use of the Service'.
[31] Directive on Unfair Terms in Consumer Contracts 93/13 EEC, OJ L 95, 21/4/93
[32] Article 3(1). The assessment of the unfairness of the terms of the contract shall be based on the nature of the goods or services and the surrounding circumstances at the time the contract was concluded.[32] The strength of the bargaining position of each of the parties, the extent to which the seller has dealt fairly and equitably with the consumer as well as issues determining whether the consumer was given any inducement to agree to the term or whether the goods or services were sold or supplied to the special order of the consumer, are all factors that according to the Directive should be taken into account when the fairness of a term is assessed. (Recital 20)
[33] Article 7(1)
[34] 'Electronic payment instruments' covers both electronic payment cards and reloadable electronic money instruments in the form of stored value cards and electronic tokens stored on network computers memory.[34] (Article 2 of the Recommendation 97/489/EC)
[35] Article 7(2) (a)
[36] Article 7(2) (d). This duty can be carried out either by the company issuing the card or by another entity appointed by the former. The entity must provide the necessary means for customers to be able to notify the loss, theft or error of the payment instrument at any time of day and night and must also provide the suitable means of proof that the consumer has given due notice. Article 9(1)
[37] The block is compulsory even if the cardholder has acted fraudulently or with extreme negligence. (Article 9(2))
[38] Article 8(1) (b). In other words, if the holder acts in a diligent way in the use and maintenance of his payment instrument and notifies however, the issuer of the loss or theft of the card, but afterward an unauthorized use occurs, the issuer is liable and must restore the holder to the position he was before the unauthorized transaction. Article 8(2) (b)
[39] Article 8(4). Article 3(3) (a) provides that the issuer is under the obligation to communicate the terms of the contract to the holder and the terms should include a description of the electronic payment instrument, including where appropriate the technical requirements with respect to the holder's communication equipment authorized for use, and the way in which it can be used, including the financial limits applied, if any. Thus, for example under these provisions and according to the Directive of Unfair Terms in Consumer Contracts as mentioned above, a term in a contract which stipulates that 'the issuer is not liable for clients' inability to use the electronic payment instrument or for delays or damage due to accidents attributed to the breakdown or failure of different devices such as EPOSs (Electronic Point of Sale) or other machines connected to the operation of the payment instrument' should be considered as an unfair term.
[40] Article 5(a)
[41] Article 5(b)
[42] Article 6(1)
[43] Articles 6(1) and 6(2)
[44] The cardholder is not in breach of his contract with the issuer if other people are aware of his personal identification number and use the payment instrument. The only consequence is that the holder will possibly be liable to the issuer and therefore liable for the costs of any transactions carried out.
[45] Directive 2000/46/EC of the European Parliament and of the Council of 18 September 2000 on the taking up, pursuit of and prudential supervision of the business of electronic money institutions. In: Official Journal of the European Communities of 27 October 2000, L 275, 39-43. http://europa.eu.int/eur-lex/en/lif/dat/2000/en_300L0046.html.
[46] Article 4, Directive 2000/46/EC
[47] Articles 4(1) and 4(2)
[48] Edgar, Electronic Commerce Legal Issues Platform: '*Electronic Pa*yments', ESPRIT Project 27028, 16 December 1999 http://www.eclip.org Also Lelieveldt, S., '*Why is the Electronic Money-Directive Significant'*? Electronic Payments System Observatory Newsletter, May 2001 Issue 7, http://epso.jrc.es/
[49] Thus the issuer must place an amount at least equal to its financial liabilities in one or both of the following; Assets that attract a zero credit risk (Article 6(1) (a)). Sight deposits held with Zone A credit institutions and debt instruments which are highly liquid. These must not exceed 20 times the own funds of the issuer. (Article 6(1) (a))
[50] Commission of the European Communities, Amended proposal for a European parliament and Council Directive concerning the distance marketing of consumer financial services and amending Directives 97/7/EC and 98/27/EC, Brussels, 23.07.1999, COM (1999) 385 final
[51] Recital 5
[52] Article 8a
[53] Directive 97/7/EC of the European parliament and the Council of 20 May 1997 of the protection of consumers in respect of distant contracts.
[54] Pichler, R., '*Finality of Credit Card Payments and Consumer Confidence – Different approaches in the United States and Europe'*. Electronic Payments System Observatory Newsletter, February 2001, Issue 7. http://epso.jrc.es
[55] The study has been undertaken under contract to the European Commission by a consortium of 10 European partners led by CRID, University of Namur and the IT Law Unit, Center for Commercial Law Studies, Queen Mary University of London. Facultes Universitaries, Notre- Dame de la Paix '*Study of the implementation of Recommendation 97/489/EC concerning transactions carried out by electronic payment instruments and in particular the relationship between holder and issuer'*, May, 2001

http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/parta.pdf

[56] i) There is lack of information provided by issuers to holders; ii) Information is provided in unclear and/or inaccessible way; iii) The information is sometimes only provided on or after the conclusion of the contract; iv) There is no limit to a holder's liability after notification.

[57] Paragraph IV of the definition, states that e-money is 'issued on receipts of funds on an amount not less in value than the monetary value issued'. This may imply that large value payments are not covered by the Directive. Thus for example, if an organization issues 100 EURO of electronic pre- paid value against a payment (or a load of 99, 9999 EURO, would this organization fall within the definition of the Directive and therefore within its regulatory provisions?

[58] Pitofsky. R., 'competition and Consumer Protection Concerns in the Brave New World of Electronic Money', United States Department of Treasury Conference: Towards Electronic Money& Banking: The role of Government, September, 1996, http://www.ftc.gov/speeches/pitofski/banking.htm

[59] Most of these electronic payment systems monitor the whole shopping process as well as other behavioral information about the consumer (i.e. sites and products visited, the amount of time spent in each site etc).[59] Some other e-payment systems on the other hand have the technical ability to ensure that transactions are carried out anonymously.

[60] Giannakoudi, S., (1999) '*Internet Banking: The Digital Voyage of Banking and Money in Cyberspace'* Information &Communications technology Law, Vol. 8, No. 3

[61] Some examples are Mastercard's solution for secure payment applications named SPA, the 3D secure system that has been proposed by Visa USA and also Maestro has proposed a solution based on a server side client wallet. For a more detailed analysis of the above menyion proposed systems see Lelieveldt, S., '*New Payments Authentication Methods for use on the Internet,'* Electronic Payments System Observatory Newsletter, July 2001, Issue 8.

[62] Pollard, S., *'Electronic Payment Systems: The legal Perspective'* Gilbert&Tobin, May,1996 http://www.gtlaw.com.au/pubs/elecpay.htm.

[63] Nadal, M., (1998) '*Electronic commerce: Digital Signatures and Certification Authorities'*, Editorial Civitas, Madrit

[64] JEPI was initiated by the World Wide Web Consortium (W3C) and has wide support in the IT industry for example, Cyber Cash, Microsoft, IBM, BT, France Telecom, Net Bill, Netscape Communications Corporation, Nokia. http://www12.w3.org/Ecommerce/JEPI/951218.html

[65] IOTP is supported by hardware industries (IBM), software manufactures (Netscape), banking industry (Canadian Imperial Bank of Commerce) and payment systems companies (Cyber Cash, Mondex International, DigiCah), http://www.opt.org .CEPS was released to the public in March 1999 and has been signed with organisations in 22 countries. For more information see Europay International '*Common Electronic Purse Specifications'* http://www.europay.com/smartcard/Smartcard_ceps_page.html

[66] One example is the Which Online WebTrader scheme that requires the e-merchant to display their logo as an indication of their compliance with the code of conduct. The German Trusted Shops scheme operated by Gerling Insurance proposes free insurance of a broader scope for consumers shopping within its trust seal area. The consumer can claim insurance in cases of non-delivery of the goods within 30 days, for non-refund of advance payment within 30 days after returning the goods, and for fraudulent use of credit card details up to 50 pounds.

[67] Mitchell, J., (1998) '*Electronic banking and the Consumer: The European Dimension'*, (London: Policy Studies Institute) p.37

[68] Banking ombudsmen programmes currently operate in Belgium, Canada, Germany, Italy, Netherlands, Switzerland, Australia, New Zealand. Giannakoudi, S., (1999) '*Internet Banking: The Digital Voyage of Banking and Money in Cyberspace'*, Information &Communications technology Law, Vol. 8, No. 3

[69] Giannakoudi, S., (1999) '*Internet Banking: The Digital Voyage of Banking and Money in Cyberspace'*, Information &Communications technology Law, Vol. 8, No. 3; Group of Ten, Electronic Money: Consumer Protection, Law enforcement, supervisory and cross borderissues,April1997http://www.bis.org/publ/gten01.pdf

[70] http://www.amazon.co.uk. Amazon.de provides the same guarantee as the British up to 100DM along with further insurance for returning goods worth more than 40EURO. http://www.amazon.de

[71] Group of Ten, '*Electronic Money: Consumer Protection, Law enforcement, supervisory and cross border issues'*, April 1997http://www.bis.org/publ/gten01.