Institute for
Prospective Technological Studies
Directorate General Joint Research Centre
European Commission

Building Security and Consumer Trust in Internet Payments

– The potential of "soft" measures –

Background Paper No. 7
Electronic Payment Systems Observatory (ePSO)

April 2002

Clara Centeno

EUR 20278 EN

IPTS, Edificio Expo-WTC,
C/ Inca Garcilaso, s/n, E-41092, Seville, Spain
Tel: +34 954488281, Fax: +34 954488208
URL : http://epso.jrc.es/

European Commission

Joint Research Centre (DG JRC)

Institute for Prospective Technological Studies
http://www.jrc.es

Legal notice

Neither the European Commission nor any person acting on behalf of the Commission is responsible for the use which might be made of the following information.

Report EUR 20278 EN

Abstract

Lack of security and consumer trust in Internet payments (I-payments) has been repeatedly reported as one of the most important factors hindering the development of e-commerce.

This seventh ePSO background paper focuses on the nature and size of the I-payment fraud problem, and, recognising the importance of the "human factor", it analyses the potential that "soft" or non-technology based measures may have in increasing I-payments security and consumer trust in I-payments.

Most consumer surveys show that consumers' lack of trust is linked to concerns on the security of payment data - mostly credit cards - and misuse of private data. However, consumer survey statistics from the available US consumer complaint registration centres report that the major problems reported in 2001 were auction fraud, products and services not as expected or products never delivered, while credit card (I-payment) fraud accounted only for 5-9% of the complaints. Therefore, a distinction between e-commerce fraud and I-payment fraud needs to be made.

Investigation into I-payment fraud shows a lack of coherent, accurate and publicly available sources of information. Nevertheless, the analysis of available information indicates that although the volume of reported fraud is relatively small (estimated by credit card schemes at 0.025%-0.035% of the total e-commerce sales volume) and affecting less than 2% of consumers, it is expected to grow significantly with the development of e-commerce, card fraud in general, cybercrime and identity theft. Furthermore, striking levels of 75% - 95% of consumers surveyed have concerns about credit card data security and privacy.

An analysis of the risks related to Internet shows that this media appears to offer an easy environment for the perpetration of fraud, due to a number of reasons such as its anonymity and easy access, the lack of risk awareness, the lack of cyber-security skills and the complex legal prosecution process for low value cross-border transactions. In this environment, a number of on-line payment risks are identified such as the risk of fraudulent merchants charging for unauthorised transactions, the risk of payment or identity data theft, the risk of misrepresentation and the risk of consumers fraudulently denying transactions.

In order to increase I-payments security, the role of "soft" measures is analysed, with a focus on fraud prevention. The particular role risk awareness and security education of

service providers, merchants and consumers can play is analysed, as well as the current barriers to increasing the level of security and the potential role of policy makers and regulation in overcoming these barriers.

In order to increase consumer trust, a broader perspective is taken, including elements of the complete shopping experience. An analysis of the nature of trust distinguishes between initial trust (necessary for consumers to make their first purchase) and maintained trust (for consumers to make further purchases). The different factors that build both initial and maintained trust are identified. These range from pre-interaction factors (i.e. brand reputation, advice from trusted sources of information), through to user interface factors (i.e. web design and usability), site information factors (i.e. merchant information, data protection and security policy statements), purchase interaction factors (i.e. clear pricing, security seals of approval, alternative methods of payment), and a positive user experience. Finally, the role of consumer awareness and education on risks and protective measures, the limitation of consumer liabilities in case of fraud, the provision of redress mechanisms, and the use of merchant trust marks as trust building measures are analysed.

A number of questions, which require further analysis, arise:

- Is there a need for a European e-commerce central fraud reporting point?
- Could the mismatch between the strong concerns of consumers about security and privacy and the real risks indicate the existence of *other* concerns beyond security?
- In promoting security, could merchant trust marks play a role in increasing consumer awareness and demand for security? What role could security standards or training play?
- Would the promotion of cybercrime law(s) among the general public be an effective measure in the short-term in decreasing “friendly fraud”?
- How could the consumer’s perception of e-commerce risks be adjusted and responsible behaviour encouraged? In building risk awareness among consumers, how could an increase of consumer’s security concerns and fraud be avoided?
- Could reputation systems used in auctions be useful for B2C e-commerce?
- Would credit card schemes be a candidate for cross-border and global ADR?

CONTENTS

1 INTRODUCTION

1.1 THE ROLE OF THIS PAPER

The lack of security and consumer trust has been repeatedly reported as one of the most important factors hindering the development of e-commerce. In addition, most consumer surveys show that consumer lack of trust in e-commerce is linked to concerns on Internet payment data security and misuse of private data.

Available consumer survey statistics from the two US consumer complaint registration centres show that the major problems reported in 2001 were auction fraud, products and services not as expected or products never delivered, while credit card (I-payment) fraud accounted for 5-9% of the complaints. Therefore, a distinction between e-commerce fraud and I-payment fraud needs to be made.

This seventh ePSO background paper focuses on the nature and size of the I-payment fraud problem, and, recognising the importance of the "human factor", it analyses the potential that "soft" or non-technology based measures may have in increasing I-payments security and consumer trust in I-payments.

The paper starts with an analysis of the nature and size of I-payment fraud, as a first step to understanding the need for counter measures. E-commerce fraud and I-payment fraud are distinguished, difficulties in the assessment of fraud are reported and findings on the level of fraud, its nature and its trends, as well as its impact on market players are presented. Finally, analysis of risks related to Internet and in particular to on-line payments is made.

In the following chapter, a range of "soft" measures for building on-line payment security is analysed, with a focus on fraud prevention, awareness and education of all actors.

Finally, in considering consumer trust, a broader perspective is taken, which addresses the overall on-line shopping experience of consumers, the *nature of trust*, its relation to *risk* and *reliance*, and, the factors that contribute to building trust. A range of trust building measures is then discussed including consumer awareness and education, the limitation of consumer liabilities in case of fraud, the provision of redress mechanisms, and the use of merchant trust marks.

Open questions

A number of questions arise which require further analysis:

- Is there a need for a European e-commerce central fraud reporting point?
- Could the mismatch between the strong concerns of consumers about security and privacy and the real risks indicate the existence of *other* concerns beyond security?
- In promoting security, could merchant trust marks play a role in increasing consumer awareness and demand for security? What role could security standards or training play?
- Would the promotion of cybercrime law(s) among the general public be an effective measure in the short-term in decreasing "friendly fraud"?
- How could the consumer's perception of e-commerce risks be adjusted and responsible behaviour encouraged? In building risk awareness among consumers, how could an increase of consumers' security concerns and fraud be avoided?
- Could reputation systems used in auctions be useful for B2C e-commerce?
- Would credit card schemes be a candidate for cross-border and global ADR?

2 OVERVIEW OF E-COMMERCE FRAUD AND I-PAYMENT FRAUD

In this chapter, the nature and size of I-payment fraud is analysed, as a first step to understanding the role that "soft" measures can play in building security and consumer trust. E-commerce fraud and I-payment fraud are distinguished, difficulties in assessing fraud size are reported, and the findings on the size of fraud, its nature and its trends, as well as its impact on e-commerce development, are presented. Finally, a risk analysis of the Internet environment and Internet payments is carried out.

2.1 INTERNET FRAUD, E-COMMERCE FRAUD AND I-PAYMENT FRAUD

2.1.1 I-payment fraud is a fraction of e-commerce fraud

First of all, Internet fraud should be defined. The FBI[1] defines Internet fraud as:

> *Any fraudulent scheme in which one or more components of the Internet, such as Web sites, chat rooms and E-mail, play a significant role in offering non existent goods or services to consumers, communicating false or fraudulent representations about the schemes to consumers, or transmitting victims' funds, access devices or other items of value to the control of the scheme's perpetrators.*

Focusing on e-commerce fraud, the statistics and surveys from the two US consumer complaint registration centres available[2] report that 33% of consumers had a problem with an on-line purchase in 2001. The major problems reported were auction fraud, products and services not as expected and products never delivered, while credit card (I-payment) fraud accounts for 5-9% of the complaints, affecting 2% of all the consumers. These figures indicate that e-commerce fraud does not necessarily imply I-payment fraud and that a distinction between both needs to be made.

An analysis of I-payment fraud requires consideration of the variety of instruments that consumers use when paying for e-commerce transactions (Böhle and Krueger, 2001), as illustrated in Table 1. The so called *on-line* payment instruments, such as credit cards, debit cards and credit transfers, are new or are used under new conditions (technical, procedural, legal). For example, credit cards, which are the most used on-line payment instrument with a share of 93% (Gartner, 2001), were initially conceived for face-to-face transactions. They are used on the Internet even though the payment instrument security

[1] See Abbreviations used in Appendix A

[2] FBI Internet Fraud Complaint Center (2001); Internet Fraud Watch of the National Consumer League (NCL), 2001 NCL's On-line shopping survey, carried out in US with a sample of 1003 adults, in Aug 2001.

measures for card and cardholder authentication (verification of the card's physical and security features such as holograms, signature, name and picture) cannot be applied. As a consequence, in this riskier environment, the product rules that apply differ from the face-to-face transactions: the merchant loses the guarantee of payment and becomes liable for fraud. Another example is the integration of the on-line banking credit transfer function within the shopping process that has been implemented in Finland, and provides instant payment guarantee to the merchant.

The *off-line* payment instruments, such as cash on delivery, checks, payment after invoice, money transfer and direct debits, are already used in the physical market place and/or in the distance selling market, and their use for e-commerce does not entail additional risks for the consumer or new conditions of use.

Table 1: Usage of Internet Payment Systems in four countries, July 2000[3]

Payment Systems		England	France	Germany	US
On-line(1	Credit card on-line	81%	61%	20%	88%
	Debit card on-line (PIN less)	-	-	-	1%
Off-line(1	Direct debit	-	-	19%	-
	Phone/fax in credit card	4%	-	-	5%
	Cash on delivery	-	10%	16%	-
	Billing existing account	4%	4%	14%	2%
	Check	-	12%	-	4%
Other		11%	13%	31%	-

Note 1) Classification added by author

Despite the important usage of the credit card as an on-line payment instrument, the two US consumer organisations report that the majority of purchases resulting in consumer complaints were paid for by money transfer or cheques, and only 15-28% of transactions resulting in complaints were paid by credit card.

In this paper we will focus specifically on the fraudulent use of on-line payment instruments. Other types of e-commerce fraud, however, should also be considered in an overall e-commerce risk analysis.

2.1.2 I-payment fraud and other types of fraud and crime

There is an intimate link between payment fraud committed in the physical world (counterfeit, lost, stolen and card not present) and on the Internet. In order to perpetrate

[3] Source: Gartner Group quoted in Rountree, 2001

credit card fraud, card details need first to be copied, stolen or generated by software, either in the physical world or on the Internet, so that fraudulent purchases can take place using these card data, both in the physical and in the virtual world. Card payment organisations (APACS UK, 2001; Visa EU, 2001; Gartner, 2001) report that the incidence of hackers stealing cardholder data from web sites is very low compared to other ways of criminally accessing card details (i.e. in a restaurant or looking through people's trash), and that most Internet fraud involves using card details fraudulently obtained in the real world.

Some of the I-payment fraud types could be considered as examples of *identity theft*, the act of acquiring an individual's private information (credit card number, social security number, phone number, birth date, address, bank account number, etc.) without consent and then using the acquired identity to commit fraudulent transactions (credit card fraud, phone bills, bank fraud, fraudulent loan, etc.).

Finally, computer crime, including *cybercrime*, is also strongly linked to payment fraud. It can be used, for example, as a means of stealing consumer identification and payment data, or a means of shutting down the operations of a bank payment authorisation server through a denial-of-service attack.

2.2 E-COMMERCE FRAUD FACTS AND FIGURES

2.2.1 Difficulties in assessing I-payment fraud

Investigation into I-payment fraud data has found a lack of coherent, accurate and publicly available sources of information. This shortcoming could be explained by various factors:

1. The lack of a central repository where all victims can report fraud;
2. The nature of the information:
    a. Organisations are not willing to report fraud (2002 CSI/FBI Survey on Computer Crime and Security shows that only 34% of organisations attacked reported the intrusion to law enforcement);
    b. Organisations are not always able to report fraud (card schemes are still unable to provide accurate e-commerce fraud figures as e-commerce fraudulent transactions can not be easily distinguished from other fraudulent transaction categories) and consumers are not always able to detect fraud on monthly statements, due to the often small value of the transactions;

c. Organisations have limited motivation to report fraud (not all consumer card fraud complaints are reported by card issuers, as these often write-off the transaction amount when it is smaller than the $50 estimated complaint's processing costs).

This lack of fraud figures in general, and in particular for the EU, limits the accuracy of the present report, which in addition is based, in many cases, on US figures.

2.2.2 Findings on I-payment fraud facts and figures

Based on available data from EU and US financial institutions, merchant and consumer organisations and consulting firms, an attempt to assess the size and nature of the fraud problem and its possible evolution is made hereafter.

2.2.2.1 Credit card e-commerce fraud

With e-commerce card transactions being 1% of total card transactions, e-commerce card fraud in Europe is estimated at 6-9% (VISA EU, Europay) of total card fraud in 2000 amounting $41 million, and at 5% (Europay) in 2001. In relation to sales, fraud is estimated at 0.025-0.035% of total e-commerce volume (Europay International, 2000, 2001; Visa EU, 2000).

On-line card fraud is estimated to be between 3 or even 30 times higher than in the physical world (Visa, 2000; Celent Communications, 2000; Garner Group, 2001).

The most common types of on-line card fraud reported (VISA, Europay, 2001) are:

- bogus merchants collecting card data and disappearing, charging either unauthorized transactions, transaction amounts higher than agreed or recurring transactions;
- transactions performed with stolen card data (in the physical world or obtained through intrusion in merchant servers) or data generated with software tools; and,
- consumers fraudulently denying transactions.

Another aspect of credit card fraudulent transactions, are the so-called *chargebacks.* Although often referred to the consumer complaints and refund process, chargeback is a technical term that describes a refund process between card issuer and (merchant) acquirer banks for a transaction following the violation of a rule[4]. Chargebacks are estimated to be 12 times more frequent for e-commerce than in the physical world, and 2-3 times more than for "MOTO"[5] sales (VISA). They can be due to a variety of reasons such as merchant unauthorized recurring charges (typical for adult sites) or higher amount charges, merchant's name unrecognisable in the bill, goods not as expected, goods not

[4] EC DG Internal Market "Payment card chargeback when paying over Internet", MARKT/173/2000

delivered, counterfeit fraud, cardholder fraudulently denying a transaction, etc. Due to the lack of accurate information, it is not clear to what degree this higher complaint rate is due to a lack of experience of e-tailers in remote sales (poor business practices, misleading or incomplete information to consumers and insufficient customer services), rather than to increased fraud committed by cardholders, merchants or other criminals. In all cases, consumer complaints generate high costs to banks and merchants and do affect the level of consumer confidence.

Although still relatively small, I-payment fraud is expected to grow, in line with:

- growth trends in Internet access and e-commerce;
- expected growth of card fraud in general (Europay[6] estimates a yearly increase of card-not-present[7] fraud of 94% and counterfeit fraud of 65% for 2001-2004);
- evolution and expected growth of identity theft (as presented in the next chapter);
- growth of cybercrime attacks (as presented in the next chapter).

2.2.2.2 Identity Theft

The US Federal Trade Commission (FTC)'s Consumer Sentinel database reports that 42% of consumer fraud complaints in 2001 are about Identity theft, with more than 86,000 cases reported. From these, 42% are related to credit card fraud (26% to new accounts and 10% to existing accounts), 20% to phone or utility bills, 13% to bank fraud, 9% to employment related fraud and 7% to loan fraud. Celent (2001) estimates that only 10% of identity theft is originated from Internet, but this percentage is expected to increase.

The US Treasury's Financial Crimes Enforcement Network reports an Identity theft 2001/2000 increase of cases of 50% and experts estimate it to triple between 2000-2005 with 1.5 million cases expected in the US (Celent, 2001; FTC, 2001).

2.2.2.3 Computer Crime

Highlights of the striking results of the 2002 CSI/FBI Computer Crime and Security Survey[8], are presented in Table 2.

---

[5] Distance selling transaction done via Mail Order or Telephone Order

[6] Quoted in European Card Review, edition Nov/Dec 2000

[7] A card-not-present transaction refers to a payment transaction where the merchant is not able to see the card, such as in Mail Order or Telephone Order distance selling or in Internet transactions.

[8] Based on 503 responses.

Table 2: Highlights of the 2002 CSI/FBI Computer Crime and Security Survey

Security breaches	**Penetration levels**	- 90% of respondents detected computer security breaches - 74% report their Internet connection as a frequent point of attack - 33% report internal systems as a frequent point of attack
	Type of attacks	- 40% experienced a system penetration from the outside - 20% report theft of proprietary information - 12% report financial fraud
www	**Web Presence**	- 98% of respondents have www sites - 52% conduct e-commerce on their sites

	Penetration levels	- 38% suffered unauthorized access or misuse (another 21% didn't know), of which:
		  - 25% report 1 incident
		  - 27% report 2 to 5 incidents
		  - 39% report 10 or more incidents

	Type of attacks	- 70% of sites suffered from vandalism attacks - 12% included theft of transaction information - 6% financial fraud

The 2001 Industry Survey by Information Security Magazine[9] reports that "insider"(full- or part time employees, contracted workers, consultants, partners or suppliers) security incidents such as access abuse and equipment theft occur far more frequently than "external" attacks.

Finally, the same survey reports that web server attacks have doubled in 2001 vs. 2000, a similar growth rate as reported by the CERT Coordination Center in 2001 for security breaches and attacks.

2.2.2.4 Profile of fraudsters

All criminal acts take place under the confluence of three factors: motivation (financial gain in the case of payment fraud), ability (skills, resources) and opportunity. The latter depends on vulnerability, accessibility and risk present - i.e. prosecution (Knapp, 2000).

There is little information available on the profile and behaviour of fraudsters, but some indications can be given on:

a. The fraudster *profiles*:

- organised criminals, with significant skills, resources and high financial gain motivation;
- hackers, with or without criminal objectives, with increasingly sophisticated skills and tools (CSI/FBI, 2001);

[9] Collecting information from more than 2,500 information security practitioners

- a significant increase of college students (Scambusters) and an increase of unsophisticated fraud perpetrators (Experian, 2000); the Internet seems to have become the first choice for thieves that, in another age, might have just been "petty shoplifters or locker room pickpockets";
- higher number of "insider" attacks than "external" Internet attacks;
- what could be called "friendly fraudsters", with limited skills and resources, that take the opportunity provided by the systems' vulnerability, easily available tools, lack of ethics and low or no prosecution risk;
- higher percentage of individuals – 76% of total alleged fraud perpetrators reported by the IFCC (2001a) – as opposed to businesses;

b. The *environments* where fraudsters do act:

- inexperienced merchants with no or limited risk management tools;
- stores that sell high value items, digital contents or items easy to re-sell (jewellery, electronics);
- auctions, which represented in the US between 64% and 87% of consumer complaints in 2000 (NCL, IFCC, eMarketer[10]), decreasing to 43-67% in 2001 (NCL, IFCC);

c. The fraudsters' pattern of *behaviour*:

- perform above average transactions, buy several of same item, do rush orders (ready to pay a lot for expedited delivery), do overnight orders, use free e-mail address or free web based address, request 'bill to' address different than 'ship to' address or international delivery address, use one single delivery address and multiple cards or use multiple cards from a single IP address;
- act as bogus merchants.

These figures point at the significant proportion of individuals perpetrating fraud, as opposed to businesses.

2.2.2.5 Impact of fraud on consumers

Public opinion research group Ipsos-Reid Group Inc reports, according to a survey (2001) of 8,500 adults in 16 countries, that less than 1% have reported on-line payment fraud. Similar figures are provided by the BizRate survey (2000) of 13,500 consumers, reporting less than 2% experiencing credit card number theft, by the US NCL 2001 Online Shopping Survey with 2% of consumers reporting credit card number stolen and used

fraudulently, and the IFCC (2001b) with less than 1% of fraudulent auction transactions. EBay reports that confirmed fraud cases are less than 0.01% of transactions.[11]

Despite this relatively low percentage of fraud cases, most consumer surveys show that consumer lack of trust in e-commerce is linked to concerns on payment data security and misuse of private data. The Ipsos-Reid Group survey (2001) reports that 75% of consumers are concerned about the potential of on-line fraud, the Gartner Group (2000) reports that 95% of users are very or somewhat concerned about privacy/security when using credit card numbers on the Internet, and Harris Interactive (2000) reports that 6 in 10 respondents fear credit card theft. There is, however, little available information on the levels of other types of consumer concerns (goods not delivered or not matching the order, etc).

Nevertheless, it is interesting to note that another consumer survey (EcaTT, 1999) of 7,700 individuals aged 15 and older in 10 EU countries provides different results. It reports that fraud, as a major barrier to e-commerce development, comes well after "equipment missing", "product unsuited", and "lack of comprehension" in order of importance.

These figures show that there seems to be a mismatch between the levels and nature of consumers' concern and the real risks of e-commerce fraud and credit card on-line fraud.

2.2.2.6 Impact of fraud on merchants

A survey carried out in the UK by the CBI (Confederation of British Industry) in 2001[12] reports that merchants are afraid to sell on-line, with two thirds of the firms reporting having suffered a serious cybercrime attack.

Average fraud costs are estimated to be lower than 1-3% (Gartner, 2001; Celent, 2000; GartnerG2, 2002), although for high risk goods, cross-border purchases and when no risk management tools are in place, fraud size can be more than 20% (BuyDirect Inc). Interestingly, Meridien Research reports (2001) that only 30% of web retailers use anti-fraud technology.

Although a little dated, the EcaTT survey (1999) of 4000 establishments in 10 EU countries shows that security is not very influential on the decision of non-e-retailers to stay away from e-commerce. "No need" is the major reason not to sell online, followed

[10] eMarketer, 'The ePrivacy and Security Report', Jan 2001, quoted by IFCC in the Auction Fraud Report, 2001
[11] News.com, 'Hackers Can Seize eBay Billpoint Accounts', 26 March 2002
[12] With 148 respondents, 32% considering that Internet is a safe place to do B2C commerce

by “product characteristics”, “missing consumer demand”, “lack of know-how” and “costs”. According to a more recent survey[13] (2002), 69% of UK firms state that “a lack of understanding by consumers and suppliers” remains the most significant barrier to e-business development.

Therefore, despite the pressure of the media, the available figures do not provide a clear assessment on the importance of payment fraud or cybercrime as a barrier for merchants’ e-commerce development.

2.2.3 Summary of findings

The investigation on I-payment fraud shows a lack of coherent, accurate and publicly available sources. Nevertheless, the analysis of available information points to a difference between e-commerce fraud and I-payment fraud, the latter representing significantly smaller percentage of the consumer complaints (5-9%), which affect less than 2% of consumers.

However, although the volume of reported fraud is relatively small (estimated by credit card schemes at 0.025%-0.035% of e-commerce sales volume and at 5-9% of total card fraud), it is expected to grow significantly with the development of e-commerce, and with the expected growth of card fraud in general, cybercrime and identity theft. The information available on fraudster profiles points at the significant proportion of individuals perpetrating fraud, as opposed to businesses.

Despite the relatively small size of I-payment fraud, 75%-95% of consumers surveyed report concerns about credit card data security and privacy. From the merchant perspective, the available figures do not provide a clear assessment on the importance of payment fraud as a barrier for e-commerce development.

2.3 ON-LINE PAYMENT RISKS

2.3.1 Internet related risks

The reported volume of e-commerce fraud points to the Internet being riskier than the face-to-face environment. E-commerce could be looked at as a new form of distance selling, characterised by a lack of face-to-face interaction and of synchronisation of payment and delivery of goods, and in the case of payment by card, by merchant’s inability to verify the payment card’s physical and security features. Committing fraud is

[13] CBI (Confederation of British Industry) and PriceWaterhouseCoopers survey published in April 2002, quoted by NUA on “CBI: Customer confusion stopping ebusiness growth”, published on Apr 11 2002.

therefore easier than in the physical world as invoices can be left without payment after reception of goods, goods can be left undelivered after reception of payment or card payment fraud can be easily committed as "plastic" is not required, i.e., only a card number and a delivery address are needed.

In addition, the Internet has a number of characteristics that introduces new risk elements:

- The environment is a more favourable vehicle for fraudsters to communicate and act due to its anonymity, low access barriers, rapid exchange of resources such as hacking programs and credit card numbers[14] (Gartner, 2001; FBI, 2000; Lang, 1999). The possibility of committing computer facilitated crime also makes it easier to automate and commit fraud on a larger scale (Schneier, 1998; CERT/CC, 2002);
- The lack of cyber-security skills and tools: organisations often overlook significant risks, i.e. system providers do not produce systems that are immune to attack, network and system operators do not have the personnel and practices in place to defend themselves against attacks and minimise damage (Pethia, CERT/CC, 2001);
- Merchants are often small and new, with limited security skills and budget, and are selling new goods (digital content) which are more vulnerable to fraud (Experian, 2000);
- Users are more vulnerable: with increasing Internet connectivity from home and increasing PC power (available for hackers), average users know little about risks and the security tools available to protect their computers from external attacks;
- Legal prosecution is more difficult, because transaction amounts are generally low, the electronic evidence tools and skills available are very limited, legislation is not yet adapted to the Internet environment and where transactions have taken place across borders, complex jurisdictional and procedural issues may arise (Schneier, 1998; Pethia, CERT/CC, 2001; Eldon, FBI, 2002[15]).

2.3.2 On-line payment transactional risks

With a view to understanding what security measures are needed and, based on results of the analysis of fraud figures available, on-line payment risks can be classified into four categories as follows:

[14] The Coalition for the Prevention of Economic Crime – CPEC, in the US, estimates that about 3000 credit card numbers are traded in Internet chat rooms each month (ZDnet, Aug 21 2001).

[15] Quoted by ABC News Internet Ventures in "Police Flat-Footed in Cyber Crimes, FBI: Tech-Savvy Criminals Outpacing Law Enforcement", on March 20th, 2002

1. Risk of merchant mis- or fraudulent behaviour: bogus merchant carrying out data capture, disappearing and charging unauthorised transactions; charging transaction amounts higher than agreed; charging unauthorised recurrent payments.
2. Risk of identity and payment data theft for further fraudulent use on the Internet or in the physical world (purchase, fraudulent card application, account take over). Identity data can be stolen through e-mail (or even phone) scam, or through on-line unauthorised access to merchant or ISP servers, to bank servers, to consumers' PCs or to transactional data.
3. Risk of impersonation, i.e., fraudulent use of (stolen) consumer identity and/or payment data, or software generated account numbers for purchasing.
4. Risk of consumer fraudulently denying a transaction.

2.4 OPEN QUESTIONS

2.4.1 Lack of central reporting point

The lack of statistical data appears as a major obstacle to understanding the nature of fraud, its size, and to what degree it affects consumers and merchants. Consequently, in the absence of a well defined fraud target problem, the security and trust measures that market players, consumers and regulators should take, are harder to define.

While some central points have been identified in the US (FBI and NCL for consumers; Scambusters.org and antifraud.com for merchants) which provide fraud reporting services, fraud statistic information, best practices sharing, and support for fraud investigation and prosecution, no similar reporting point has been identified at European level. The question that appears is:

- Given the border-less nature of e-commerce, and in support of the European internal market development, should a neutral European central fraud reporting point be established independent of the payment instrument used, to better understand the nature and size of e-commerce fraud as a measure to build e-commerce security and consumer trust?

2.4.2 Understanding consumers' concerns and behavioural impact

A significant difference has been identified between the percentage of consumers actually affected by I-payment fraud and the percentage of consumers very concerned about the security/privacy of payment data. In addition, individuals who have never shopped on-

line, report a higher (more than double) concern regarding fraudulent use of credit card details than do those who have already shopped (BizRate, 2000).

In view of the above, together with the fact that the commercial use of the Internet is relatively new (since 1995), and as its penetration grows, many Internet users have been 'on-line' for a relatively short time period, some questions arise for additional research:

- Could consumer security and privacy concerns in general (and in particular the non shoppers' greater concerns) indicate the existence of *other* consumer concerns beyond security? Should these be assessed? Could these be linked to the lack of familiarity with the Internet technology, its complexity of use, or may be due to the lack of value perceived or lack of knowledge of what can be bought on the Internet?
- As a high level of concern can be observed for both consumers that do not buy on-line and those that actually do, what is the real impact of consumers' security and privacy concern on their shopping behaviour?

3 MEASURES FOR BUILDING ON-LINE PAYMENT SECURITY

In this chapter a number of measures for building on-line payment security are analysed. Due to the impact of fraud on consumer trust and to the complexity of legal prosecution, a stronger emphasis will be put on *fraud prevention* as the first step in reducing fraud.

Recognising the importance of the human factor in building security, special attention is paid to non-technology based or "soft" measures.

During the analysis, the different fraudster profiles are taken into account. While some measures may help to prevent fraud in general, others may address more efficiently specific types of fraud: strong consumer awareness could be regarded as a measure against organised crime and the promotion of cybercrime law as a measure against "friendly fraud".

3.1 THE ROLE OF "HARD" MEASURES

Different "hard" or technology-based security measures are proposed by card schemes and banks to address the on-line payment fraud risks consumers and merchants do face. These aim to provide data confidentiality and integrity, consumer and merchant authentication and non-repudiation for each individual *transaction*. The solutions range from the cheap and easy SSL, complemented by a real time authorisation by the issuer, address and CVV/CVC2 validation, the use of passwords and user Ids, virtual and pseudo card numbers, 3D-model based solutions, SET and EMV smart cards. Other actors such as payment service providers and mobile operators add a layer of security by imposing registration and monitoring procedures of both consumers and merchants (i.e. Paypal), providing pseudonymity, separating the authentication process (i.e. using the mobile phone) from the Internet purchase process and /or generating a consumer order confirmation with the use of a PIN code (i.e. via the mobile phone). Though SSL has been widely adopted for confidentiality and integrity of data exchanged, the general adoption of the other measures is questionable due to their diversity and lack of interoperability, the lack of incentives for the different players and the potential impact on the cardholders (Centeno, 2001).

The security of the *environment* in which on-line transactions take place such as the technical infrastructure of the consumers, merchants, banks and service providers also need to be considered. In this area, payment schemes are promoting with security standards and best practice the increase of information security at banks, merchants and service providers.

In addition, the protection of consumers' PCs should be stressed. Often overlooked, the consumers' PC vulnerability is considered one of the major future security threats by some security experts (Spafford, 2002). An example of a measure to decrease this threat's risk is the US National Cyber Security Alliance, created as a partnership of government and industry members aligned with the common goal of educating Americans on the need for (individual) computer security as an aspect of homeland defence.

3.2 THE ROLE OF "SOFT" MEASURES

Security is a process, not a product. It involves the human factor and is as weak as the weakest link. Humans themselves may be the weakest link in securing information systems, reports a panel of security experts.[16] For example, the strongest cryptography will not help if a user compromises the password. Even more, social engineering attacks where secret information is obtained by talking to people rather than through a computer, are often the most damaging of any attack (Schneier, 2000).

The important role of soft measures is also illustrated by a security report presented to Congress in Feb 2002[17], which disclosed that the IT security frameworks of more than 50 government agencies suffer from similar weaknesses. The most common weaknesses cited are in the areas of effective management, organisation, education, awareness and procedures, and not technology.

In this chapter, the role of "soft" security building measures to prevent fraud such as awareness, education and cybercrime law is analysed.

3.2.1 Service providers awareness and education

Table 3 (overleaf) presents common general security mistakes that people commit in relation to computer security (SANS, 2001; Computerworld, 2001). CEOs, CIOs and senior management overlook the risks of both insiders and external attacks. Two surveys show that more than 90% of 1,400 CIOs believe their networks are safe from internal and external security breaches[18], and that the risk of external attack is higher than internal[19], while security surveys (CSI/FBI 2002) provide different vulnerability facts, as we described in the previous chapter.

[16] Computer Security Institute Conference, 31st Oct 2001
[17] Office of Management and Budget security report required under the Government Information Security Reform Act (2000), US.
[18] Carried out by RHI in Jan 2001
[19] KPMG 2001 Global e.fr@ud.survey shows that 79% of the 1253 respondents from public and private organisations in 12 countries believed that a breach in their e-commerce system would most likely be perpetrated through the Internet or external access.

Table 3: Common security mistakes

User Security Mistakes
▪ Opening unsolicited e-mail attachments, without verifying source or checking content ▪ Failing to install security patches (specially Microsoft Office, Internet Explorer and Netscape) ▪ Installing screen savers or games from unknown sources ▪ Not making and testing back-ups ▪ Using a modem while connected through a LAN ▪ Writing password in Post-it notes ▪ Leaving the machine on, unattended ▪ Poor password selection ▪ Talking (about confidential data like passwords) ▪ Leaving laptops unsecured and unattended
Senior Management Security Mistakes
▪ Assigning untrained people to maintain security and providing neither training nor time to learn ▪ Failing to see the consequences of poor security ▪ Failing to deal with the operational aspects of security (i.e. fixes follow-up) ▪ Relying primarily on a firewall for security ▪ Failing to realize how much money their information and organisational reputations are worth ▪ Authorizing reactive short term fixes, so problems re-emerge rapidly ▪ Pretending problems will go away if they are ignored

In the task of building I-payments security at service providers, i.e., reducing identity or payment data theft, in order to protect communication and information systems and data stored, the following appear as key building blocks:

- awareness of security risks at all organisational levels,
- education of employees and end users, and,
- good internal security managerial, organisational and operational procedures.

3.2.2 Consumer awareness and education

Consumers can play a significant role in reducing merchant fraud risk by taking an active and cautious attitude when shopping on-line. A number of recommendations are provided by some international consumer sites (Scambusters, Consumers International, US NCL, FBI) covering both fraud prevention measures and consumer protection measures in case of dispute. In relation to fraud prevention, some recommendations are listed:

- verify merchant's identity, company information (name, physical address and phone number) and merchant's use of codes of conduct or trust marks;
- be suspicious about very advantageous deals, from free email addresses;
- check seller's reputation (in auctions);

- check if SSL protocol is used for data protection;
- check company's security policies and tools used, and in particular for personal data protection;
- check privacy policy and how personal details may be used;
- look for insurance for buyers;
- pay on delivery or with credit card as this generally provides refund rights;
- ask your bank for a random card number option;
- consider using an escrow service;
- keep a trace (e-mail), print order screen, terms and conditions and any communication with merchant.

To fight against Identity theft, education could play a role in increasing consumers' responsibility for keeping personal data secure in the physical and virtual world. It could teach them to be aware of the risks, avoid phone and email scams, minimise the amount of data provided to web merchants and use a pseudonym when possible.

Finally, consumers also have a significant role in identifying fraud promptly, by analysing their bank and card service providers' statements in detail. Faster fraud detection can contribute to fraud prevention by blocking a lost, stolen or counterfeited card or other stolen identity data, and by identifying a fraudulent merchant or a fraud pattern.

3.2.3 Merchant awareness and education

The contribution merchants can make to fraud prevention by screening fraudulent transactions is often overlooked. The lack of consumer authentication by issuer banks combined with merchants' liability for fraudulent credit card transactions have motivated the development of merchant-based authentication solutions, reducing on-line fraud by 66-80% (ScamBusters, Gartner 2001 Survey). These solutions sometimes combine "hard" and "soft" measures. They include address validation (in the US and UK), on-line authorisation, customer follow-up (e-mail confirmation, etc), customer history database consultation, fraud scoring systems, customer data format and content editing rejecting orders with incomplete information, proof of delivery to the verified billing address, domain site check, application of additional measures for high risk purchases (call customer, ask for issuer bank and phone number, ask for exact name on credit card), state on web site that anti-fraud measures have been put in place, etc.

Merchant awareness and education is thus important and, to support it, some US organisations have been identified to provide merchant information of fraud types, statistics and best practices (Antifraud.com, Scambusters.org).

3.2.4 Responsibilities and hurdles in building security

In spite of the e-commerce security weaknesses and their impact on e-commerce development, market observation indicates that increasing the current level of security is not a straight forward process. Different barriers are identified:

- Consumers do not seem to be ready to pay for increased security and seem to be more interested in cheap goods than in secure sites (Jupiter and Ipsos, 2000);
- Merchants may be reluctant to invest significantly in a diversity of more secure solutions. Furthermore, consumer convenience and speed outweigh the advantages of secure but complex payment instruments. Merchants estimate they would lose 8% of customers if they install secure but complex payment solutions. The cost of these solutions would be then higher than the fraud cost they bear with less secure solutions (T. Arnold CTO of CyberSource, 2001);
- Most banks have invested “little” so far in building on-line security to reduce fraud in e-commerce, and have failed to promote a unique architecture for secure I-payments;
- Banks, service providers and merchants lay themselves open to attack and data theft, sometimes jeopardising the rights of their customers;
- Given the lack of consumer demand, software companies have little incentive to invest in more secure products, which require longer time to market, higher costs and complexity. They therefore sell software products with security holes, and knowingly fail to reform their architectures to make them less vulnerable (Schneier, 2002; US National Research Council – Computer Science and Telecommunication Board, 2002).

3.3 OPEN QUESTIONS

3.3.1 Potential role of policy makers in increasing security

Despite the reported lack of security of e-commerce, its current level does not seem to stop a number of consumers from shopping on-line. However, if adoption of e-commerce by the public at large is to be achieved, further policy actions may be needed, as the

increase of the level of e-commerce security currently presents a number of significant barriers, described previously.

The following questions would require additional analysis and discussion:

- Will we observe a self-regulated process in which, a higher consumer awareness will create higher demand for merchant security, motivating suppliers to invest in more secure products?
- Could merchant trust marks play a role in promoting security as a value, increasing consumer awareness and demand for security?
- Will the (planned) transfer of credit card fraud liability from merchants to issuer banks, motivate merchants sufficiently to invest in new secure solutions? Will it motivate issuer banks to invest in more secure solutions?
- What role could hardware and software security standards (such as those in other industry sectors) play?
- Should a kind of liability be allocated to software vendors or to organisations vulnerable to data theft?
- What role could security training play?

3.3.2 The short-term potential role of cybercrime law

A crime can be defined as the commission of an act which violates an established law (Knapp, 2000). Since November 2001, 33 countries have signed the Council of Europe's Convention on CyberCrime[20], the first international treaty on crimes committed via the Internet and other computer networks. It deals particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

In line with this Convention, the European Commission has adopted (23 April 2002) a proposal for a Council Framework Decision on "Attacks against information systems" (including hacking, viruses and denial of service), which seeks to approximate criminal law across the EU to ensure that Europe's law enforcement and judicial authorities can take action against this new form of crime. This proposal, however, does not cover computer assisted malicious activities such as payment fraud.

[20] Opened for signature in Budapest on 23 November 2001

In parallel with these foreseen law changes, many people see computer crime and other electronic crimes as mainly a moral issue. For example, many citizens would consider it a criminal offence to steal a CD from a physical store, and may not, however, consider that copying a CD from a friend or downloading music titles (using distributed P2P platforms such as Audiogalaxy, KaZaA) through the Internet to be equally criminal, although, according to the CyberCrime Convention, it would be.

While current EU and international activities will impact national legislation on cybercrime, the question is how long will it take to change public's perception of crime. And in relation to this, a question that would require further analysis is:

- Would the promotion of cybercrime law(s) among the general public be an effective measure in the short term in decreasing "friendly fraud"?

3.3.3 Communicating risk to consumers

Current levels of consumer concern about the risk of fraudulent use of credit card numbers on the Internet seem disproportionate in relation to the real risks. The media is often blamed[21] for this perception. However, some research results question the real media influence on consumer risk perception, particularly as regards personal risk vs. general risk, where direct information from people about experience and personal experience seem to be a much stronger factor (Wahlberg, Sjoberg, 2000).

According to available surveys, consumers disregard other types of e-commerce risk and consequently fail to behave responsibly to prevent fraud. While consumer concerns point at payment data security and privacy, NCL's 2001 On-line Shopping Survey shows that nearly one third of consumers had a problem with an on-line purchase, 13% report that products and services received were not as promised, 5% that the product was not delivered and 3% that the seller tried to charge more than the original agreement.

Risk communication is a sensitive task, subject to potential undesired effects, as other sectors such as food safety have shown (Powell, 2000). This also applies to e-commerce, and dialogue among actors (scientists, industry, citizens, policy makers and media) should follow the same accepted framework of relationship between science, technology and governance[22].

[21] Published in 'The Industry Standard' on Jun 13 2001, reporting from market analysis firm Jupiter Media Metrix.

[22] Debated during the Conference: "Science and Governance in a Knowledge Society: The challenge for Europe", 16-17 October 2000 in Brussels organised by EC DG JRC.

The following concrete questions regarding risk communication would require additional research:

- How could the consumer's perception of e-commerce risks be adjusted and responsible behaviour encouraged?
- In building risk awareness among consumers, how could an increase of consumer's security concerns and fraud be avoided?
- Could lessons be learnt from other sectors?

4 BUILDING CONSUMER TRUST

In this chapter a consumer perspective is taken in an attempt to understand the nature and the different types of trust, its relation to risk and reliance and the factors that contribute to building consumer trust. Then a selection of trust building measures is analysed such as consumer awareness and education, the limitation of consumer liabilities in case of fraud, the provision of redress mechanisms, and the use of merchant trust marks.

Though the focus in previous chapters has been limited to I-payment fraud, the analysis of consumer trust requires a more global approach including elements of the complete shopping experience.

4.1 DEFINITION OF *TRUST* AND ITS RELATION TO *RISK* AND *RELIANCE*

Buying on the Internet involves a number of *risks* for consumers such as information asymmetries, lack of personal interaction, limited ability to inspect the desired product and the fear that the company they do business with today might not be there tomorrow (Einwiller, Geissler, Will, 2001; Jarvenpaa, Tractinsky, 1999).

Trust could be defined as the consumer's willingness to risk the loss of time, money and personal data (Nielsen Norman Group, 2000), in a situation involving uncertainty. It is determined by the level of perceived risk, the importance of the goal to be achieved (benefits, added value) and the willingness of individuals to accept risks. This implies that merely increasing the level of consumer trust, does not necessarily imply that consumers will buy more; other needs also have to be met for consumers to move over their trust threshold and make a purchase, such as the availability of *attractive goods and services*.

The aim of building consumer trust in e-commerce is twofold: to encourage potential buyers to purchase for the first time and to encourage those who have already bought once to continue to do so. Consequently, two types of trust can be defined, *initial trust*, which will allow a consumer to shop for the first time at a given merchant site and *maintained trust*, which affects the long-term relationship allowing the consumer continues shopping (Egger, 2001).

Reliance is also associated with the concept of trust (Pichler, 2000). If trust can be defined as a consumer's expectation that things will go all right, reliance is a consumer's belief that although things might go wrong, they can be fixed.

4.2 UNDERSTANDING CONSUMER TRUST BUILDING FACTORS

4.2.1 Building factors of "initial trust"

Research in this area[23] points to a number of factors that play a role in building "initial trust". An analysis of these factors, following the consumer chronological shopping experience, shows that, in building "initial trust", security assessment and payment procedures take place very late in the evaluation of trustworthiness by the consumer, just before placing an order.

Table 4 lists the identified consumer trust building factors divided into pre-interaction, user interface, site information and purchase interaction factors (following the chronological shopping experience).

Table 4: Consumer "initial trust" building factors

Pre-interaction factors	- Brand reputation and awareness - Previous own experience in the off-line world - Advice or experience from trusted sources of information (word of mouth, traditional media)
User Interface factors	- Design, image, professionalism - Usability, effective and easy navigation - Native language
Site information factors	- Transparency - Company information (including physical address and contact data) - Customer service contact numbers - Link to trusted companies (for small or web based merchants)
Payment / security related	- Data protection and data privacy statements - Security policy statements
Purchase interaction factors	- Contractual terms and conditions - Clear pricing offer (including delivery costs, taxes, etc) - Clearly stated return policy (procedure, costs, reimbursement) - Ability to back-out of a transaction
Payment / security related	- Security seals of approval (e.g. credit card logos, trust marks) - Provision of alternative payment methods with different risk levels for consumers (cash on delivery, credit card, etc) - Use of up-to-date technology (encryption) - Detailed step-by-step payment procedures

[23] Cheskin, 2001; Egger, 2001; Einwiller et al., 2001; Harris Interactive, 2001; Jarven Paa and Tractinsky, 1999; Klasen, 2001; OECD; GBDe.

4.2.2 Building factors of "maintained trust"

For the development of e-commerce, it is important that after the first purchase, the trustworthy environment is maintained through a positive experience, to encourage further purchases. Although building factors of initial and maintained trust have some common aspects, for the latter, the complete shopping experience needs to be addressed.

Essentially, a positive experience will be created by the application of good business practices and providing tools and procedures for efficiently solving potential problems. These business practices are addressed by the EC Distance Selling Directive, the OECD Guidelines for Consumer Protection in the Context of Electronic Commerce, and also by the different trust mark schemes developed. Table 5 below lists some of these good business practices[24], with particular attention to the security and payment aspects.

Table 5: Good e-commerce business practices

General commerce

- *Fair* business, advertising and marketing *practices*, taking into account the age, knowledge and maturity of intended audience, in particular, children
- Provide *merchant information*: identity (legal and business name), physical address, contact information
- Provide relevant qualitative and quantitative *information on goods and services*, related costs (including delivery and taxes), currency, offer validity period, geographic restrictions
- Provide information on applicable *after-sales services and guarantees*
- Provide clear and printable *terms and conditions* of the contract
- Provide information on *goods availability* and *delivery time*
- Provide a *confirmation process* to allow consumers to review, cancel, modify, and / or record the purchase order
- Provide timely *order confirmation* with complete detailed order information

Payment and security related

- Provide information on *payment types*, charges, discounts and *billing* period
- Provide information if a *right of withdrawal* exists, related conditions, procedures and costs
- Provide information on *return policy* and related costs
- Provide information that *suspect orders* may be rejected
- Have a *privacy policy* and communicate it to the customer
- Have a *security policy* on consumer personal and transactional data and communicate it
- Provide information on the *security and authentication systems* used
- Have high standard technological means to ensure *authenticity* and *confidentiality of financial transactions and payments*, and communicate them to consumers
- Provide *on-line access to an in-house complaint system*, which is fair, effective, transparent and confidential
- Provide information of adhering *alternative dispute resolution scheme* and contact data

[24] Sources: EC Distance Selling Directive 97/7/EC, OECD Guidelines for Consumer protection, BEUC and UNICE e-confidence project trust mark requirements, and author's analysis.

4.3 MEASURES TO BUILD CONSUMER TRUST

In this section, a range of measures to build consumer trust and reliance are presented, such as consumer awareness and education, limitation of consumer liability in case of fraud, the availability of redress mechanisms and merchant trust marks. The last two measures are included in the EC e-confidence strategy to encourage consumer confidence in electronic commerce, initiated by the DG Health and Consumer Protection.

4.3.1 Consumer awareness and education

The mismatch between consumer B2C e-commerce risk perception and the real risks has already been pointed out. Another illustration is the auction market. Though 65% of consumer complaints in 2000 relate to auction fraud, according to NCL's On-line Auction Survey (2000)[25], only 50% of the bidders would 'always' check the sellers' reputation, 37% would 'usually' check, and only 53% of the respondents would be reluctant to bid if there is no information available on the auction site about a seller's track record. No more than 6% have used escrow services in auction sites, 42% due to lack of knowledge and 30% due to lack of risk concern.

This lack of consumer awareness of the actual level of risks, of risk reduction measures and of available protection mechanisms is a major target of consumer protection.

Therefore, in addition to the measures to prevent fraud listed in the previous chapter, consumer protection websites suggest additional prevention measures, such as checking information on:

- how to cancel an order;
- how to return a good for a refund and the related costs;
- complaint procedures and contact details;
- detailed costs including delivery and taxes;
- delivery time;
- warranty details and procedures;
- after-sale customer service (for durable goods) and procedures;
- relevant country legislation for cross-border purchases.

It would be interesting to see if efforts to increase consumer awareness lead to enhanced merchant business practices, as a consequence of consumer demand.

[25] Harris Interactive QuickQuery^{SM}, conducted in US in December 2000, with 2196 respondents of 18+ of age, with support of Tradenable, a major provider of escrow services

4.3.2 Limitation of consumer liabilities in case of I-payment fraud

The limitation of consumer liability in the case of I-payment fraud is an important factor in building consumer confidence. This limitation will depend essentially on the payment instrument used and the legal contracts between the consumer and the payment instrument provider.

The EC (non-binding) Recommendation 97/489/EC on electronic payment instruments, Article 6, limits the liability of the holder:

1) in case of loss or theft up, to 150 Euro,
2) as soon as the holder has notified the issuer, he/she is not thereafter liable for the loss arising in consequence of the loss or theft of his/her electronic payment instrument,
3) the holder is not liable if the payment instrument has been used without physical presentation or electronic identification (of the instrument itself), as the use of a confidential code or any other similar proof of identity is not, by itself, sufficient to entail the holder's liability.

The Recommendation also outlines the liabilities of the issuer, in Article 8, for:

1) the non execution or defective execution of the holder's transactions, and,
2) transactions not authorised by the holder.

However, in spite of these consumer protection provisions, a recent study carried out by the EC to identify the degree of implementation of the Recommendation shows that "there is a substantial level of non-compliance in respect of the obligations and liabilities of the parties to the contract". Common examples of non-compliance are the failure to limit a holder's liability after notification, failure to restrict liability when the electronic payment instrument is used without physical presentation or electronic identification and failure to provide for the liability of the issuer for defective or non-executed transactions. Consequently, measures to address these shortcomings will be foreseen in a new Directive currently under preparation.[26]

4.3.3 Redress mechanisms

After purchase and payment have taken place, cardholders need cost-effective redress mechanisms to resolve problems like unauthorised charges (fraud), undelivered or unsatisfactory purchases and/or billing errors, in order to build reliance. According to the

[26] Announced at ePSO Final conference on 19 Feb 2002, by J-C. Thébault, EC, Director Financial Institutions, DG Internal Market.

OECD (2001), the number of consumer related complaints with regard to Internet is increasing, being the most common e-commerce complaints the failure of merchants to deliver goods on time, if at all, non-disclosure of charges/costs, insufficient information on product attributes and inadequate complaint handling.

In addition to the option to use escrow and insurance services to reduce risk, consumers have several redress mechanisms. The following steps apply:

1) The consumer would first attempt to resolve the problem with the merchant. It is expected that the majority of problems would be solved at this stage.

2) In cases where the merchant's customer service did not satisfactorily resolve the consumer complaint, the consumer can use the refund capability linked to the payment instrument (credit cards, some direct debit schemes), if provided by the contractual terms and conditions that govern the payment instrument.

3) Although consumers have the right to seek redress through the courts (described below), most transactions will be low value. This option would therefore be generally inefficient due to the related costs, difficult access and long resolution time, both at a national level and for cross-border cases (accentuated in this last case). As a result, out-of-court alternative dispute resolution mechanisms (ADR) are necessary. Different types of ADR mechanisms exist (Chawdhry and Wilikens, 2002), accessible through Online Dispute Resolution (ODR) systems services, and reachable from the consumer's desktop:
   - *Automated negotiation*, is an online resolution of financial disputes via negotiation. This non-binding mechanism is low cost and fast.
   - *Mediation*, is based on the intervention of a third party, the mediator, who helps the two parties find a solution. This non-binding mechanism is more expensive, takes longer than the automated negotiation, and is suitable for complex disputes, involving non-quantifiable claims.
   - *Arbitration*, is a formal process involving a third party, the arbitrator, who is actively involved in finding a solution using semi-legal procedures, and in taking a decision which is usually binding. This mechanism takes longer and is expensive, suitable for high value disputes, to be used after a failed mediation.

   For EU cross-border transactions, the recently created EEJ-Net (European Extra Judicial Network, an element of the e-confidence strategy) aims to provide practical information and support to consumers on making a claim to an ADR system in the

country where the business is located. This is achieved by using the existing European out-of-court consumer dispute resolution schemes.

Two EC Recommendations (98/257/EC and 2001/310/EC) provide principles applicable to the bodies responsible for out-of-court arbitration and mediation (respectively) of consumer disputes.

4) As a final resort, consumers have the option to use the legal tools in their own country (as the third element of the EC e-confidence strategy). This is a fundamental principle common to the legal systems of all Member States and enshrined in the Brussels Convention of 1968, which has now become the so-called "Brussels Regulation" on jurisdiction, that ensures consumers have the "safety-net" of access to justice through the courts of their own country.

4.3.4 Merchant Trust Marks

A survey carried out by Consumers International (Sep 2001) indicates that a number of essential elements of good business practices are still not in place, such as providing clear information on a number of aspects such as cost, terms and conditions and geographical service area. Also many web sites do not comply with existing laws and guidelines (EC Distance Selling Directive and OECD Guidelines on consumer protection), failing, for example, to inform the consumer on the retailer address, his right to withdraw from the contract, or after-sales warranties.

The survey points to the importance of merchant education, the definition and promotion of good business practices or "codes of conduct", and their publicity to consumers, as important actions for building (and maintaining) trust.

Merchant trust marks and related codes of conduct aim at these objectives. They consist of measures to foster consumer trust and confidence in the relationship between businesses and consumers in on-line commercial transactions and support competition by offering a branding tool for SMEs and on-line retailers. Branding is particularly important for SMEs or new on-line retailers which, unlike big and well established organisations in the physical marketplace, can not use their brand in order to build trust.

In December 2001, as part of the e-confidence strategy, the EU decided to develop a European trust mark scheme, to be elaborated by UNICE (Union of Industrial and Employers' Confederations of Europe) and BEUC (European Consumers' Organisation). This initiative aims to establish a *single* trust mark that will facilitate consumer recognition, associated good business practice principles, as well as a mechanism to

ensure that those principles are applied in practice by companies subscribing to the trust mark.[27]

4.4 OPEN QUESTIONS

4.4.1 Could reputation systems be useful for B2C e-commerce?

In auction sites, where millions of buyers and sellers meet to trade, specific mechanisms are required to build trust among trading parties. Reputation systems or feedback forums have been successfully used to build trust as the 30+ million users registered at eBay, and the 40,000 new users registered per day show.[28] In reputation systems, buyers and sellers rate and document the quality of their experience with each other, and this information is made available for future traders. The system is managed by the marketplace (i.e. eBay). Despite their theoretical and practical difficulties, reputation systems appear to perform reasonably well (Resnick, 2000).

In addition to providing information that allows buyers to distinguish between trustworthy and non-trustworthy sellers, and vice-versa, a reputation system encourages sellers to be trustworthy, and discourages participation from those who aren't (Resnick, Zeckhauser et al., 2000).

The following questions arise:

- Could reputation systems be extended from a closed community to the open B2C market as a tool to build consumer confidence (especially suitable for SMEs and web-based merchants with limited or no brand awareness and reputation)?
- Could these systems be managed/regulated by a neutral body, where consumers would provide and consult merchants' reputation?
- Would there be synergies or complementarities between merchant trust marks and these regulated reputation mechanisms?

4.4.2 Are payment cards a candidate for cross-border and global ADR?

The availability of consumer liability limitation in case of fraud and redress mechanisms is essential for consumer trust and reliance in e-commerce. Looking at how consumers pay in the EU, it can be observed that these tend to use either off-line payment mechanisms, such as cash on delivery or payment on reception of the bill, or on-line

[27] Reference text: "David Byrne welcomes breakthrough in helping consumers shop on-line with confidence", Brussels, 10 December 2001.
[28] "The Brawn Behind Ebay's Always-On Actions", InformationWeek.com, 10 Dec 2001

payment mechanisms that provide them redress embedded possibilities, such as credit cards and direct debits (in Germany).

Generally speaking, the credit card is the on-line payment instrument that provides best consumer protection, as it provides, beyond payment, the possibility for the cardholder to dispute some or all aspects of a transaction paid for with a card, through the card issuer (chargeback) in case of over-charge, unauthorised one time or recurrent charges, undelivered or unsatisfactory goods, fraud or billing errors. However, as an EC study on chargebacks shows [29], in contrast to the situation in the US where chargebacks are a "de facto" right (based on legislation) for the cardholder [30], chargeback is not a de facto right for the European consumer. In Europe it is the card issuer who decides whether or not to launch a chargeback procedure in case of consumer complaint. Consequently the effectiveness of this method of recourse can be reduced by the existence of national rules (e.g. irrevocability in France) which are set as a barrier to the possibilities offered by the international schemes, both at domestic and cross-border level.

Consumer lack of awareness of the existence of "chargeback" has also been identified, as banks and payment service providers may be reluctant to publicise it, for fear of potential abuse.

Taking this into account, the potential role of card payment tools for redress, in a border-less EU and global e-commerce context, has been analyzed by the OECD and TACD[31] as an out-of-court dispute resolution mechanism, complementary to other ADRs solutions.

Following these studies, some questions are raised:

- Should the European Union strengthen and harmonise payment card consumer protection to use it to redress on-line disputes?
- Should payment card protection be a matter of law or regulation to provide legal certainty and consistent minimum rights for all consumers?
- Should payment card protection regarding liability limitation and chargebacks be consistent across card types (including credit cards, debit cards, stored value cards) and for domestic and cross-border transactions?
- Should payment card companies disclose to consumers their rights and the procedures to be used in disputing on-line payment card transactions?

[29] EC DG Internal Market 'Payment card chargeback when paying over Internet', MARKT/173/2000
[30] 'Truth and lending act for credit card' (Reg Z), and Electronic fund transfer act" (Reg E)
[31] Trans Atlantic Consumer Dialogue, 'Payment Card Redress and Protections', May 2001

APPENDIX A: ABBREVIATIONS USED

B2C	Business To Consumer e-commerce
CERT/CC	Computer Emergency Response Team / Co-ordination Center
CSI	Computer Security Institute
CVC/CVV	Card Validation Code / Card Validation Value
EC	European Commission
EMV	Europay, MasterCard and VISA Integrated Circuit Card Specifications for payment systems
FBI	Federal Bureau of Investigation, US
FTC	Federal Trade Commission, US
GBDe	Global Business Dialogue on electronic Commerce
IFCC	Internet Fraud Complaint Center, US
ISP	Internet Service Provider
NCL	National Consumer's League, US
OECD	Organisation for Economic Co-operation and Development
PIN	Personal Identification Number
PKI	Public Key Infrastructure
P2P	Person to Person e-commerce
SANS	System Administration, Networking and Security Institute
SET	Secure Electronic Transaction payment protocol defined by VISA and MasterCard
SSL	Secure Socket Layer
TACD	Trans Atlantic Consumer Dialogue
3D-model	Three Domain Model : Issuer, Acquirer and Interoperability Domains

REFERENCES

APACS Card Watch
Card fraud - The facts, 2001, (http://www.cardwatch.org.uk/html/card_fraud_facts.html)

Berlecon Research
Kassieren im Ecommerce - Eine Analyse relevanter Zahlungssysteme aus Händlersicht (Getting your bills paid in e-commerce). Berlin: Berlecon Research 2001, (extracts at http://www.berlecon.de/studien/zahlungssysteme/en/index.html) [Study analysing the merchant side of Internet payments. It underlines the role of those payment instruments most heavily used in the traditional MO/TO sector for e-tailers]

Böhle, Knud and Krueger, Malte – IPTS JRC European Commission
Payment Culture Matters – A comparative EU – US perspective on Internet Payments, ePSO project – Background Paper No.4, May 2001 (http://epso.jrc.es/backgrnd.html)

Bounie, David and Vaninetti, Livio
E-payments: Which Systems in Europe for the Coming Years? Issue Report N.13 June 2001, STAR - Socio-economic Trends Assessment for the digital Revolution, (http://www.databank.it/star) [Examines the competitiveness of a chip associated with the SET payment protocol – CyberCOMM – in opposition to the Secure Socket Layer communication protocol]

Caldwell, Kaye - CommerceNet
EPayments: Is the Credit Card System Failing eCommerce? Is a solution in Sight?, published in "The Public Policy Report", Vol.3, No. 5 May 2001, CommerceNet, (www.commerce.net)

CBI – Confederation of British Industry
The Cybercrime Survey 2001, Aug 2001, (www.cbi.org.uk)

Centeno, Clara – IPTS JRC European Commission
Securing Internet Payments – The potential of Public Key Cryptography, Public Key Infrastructure and Digital Signatures, ePSO project –Background Paper No.6, Nov 2001 (http://epso.jrc.es/backgrnd.html)

CERT/CC – Computer Emergency Response Team / Co-ordination Center
Overview of Attack Trends, April 8 2002, (http://www.cert.org/archive/pdf/attack_trends.pdf)

2001 Annual Report, (http://www.cert.org/annual_rpts/cert_rpt_01.html)

Chawdhry, Pravir and Wilikens, Marc – IPSC JRC European Commission
Consumer Protection and Redress in e-Payments – Issues, Policies and Technologies, IPTS Report, April 2002 (?? Name and website)

Cheskin Research, Studio Archetype/Sapient
eCommerce Trust Study, January 1999 (http://www.cheskin.com/)[This study determines the nature of those elements that communicate "trust" in e-commerce sites, be they transactional or graphical]

Trust in the Wired Americas, July 2000 (www.cheskin.com) [This study extends the learning from the initial Trust Study, and explores the dimensions of online trust in the US, Spanish-speaking Latin America and Brazil]

Computer Security Institute, US
2002 CSI/FBI Computer Crime and Security Survey, Computer Security Issues and Trends Magazine, Vol. VIII, No.1, Spring 2002, US (www.gocsi.com)

Consumers International
Should I buy? – Shopping online 2001: An international comparative study of electronic commerce, September 2001, (http://www.consumersinternational.org)

Council of Europe
Convention on Cybercrime, Budapest, 23 Nov 2001, (http://conventions.coe.int/Treaty/EN/projets/FinalCybercrime.htm)

Davis, F. D.
Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 1989. 13:3 (September), 319-340

EcaTT – The International Research Project Electronic Commerce and Telework Trends
Diffusion and Adoption of Electronic Commerce – What is Switzerland's Position in the International Comparison?, June 2000 (http://www.ecatt.com/ecatt)

EcaTT Final Report, August 2000, (http://www.ecatt.com/ecatt)

Egger, Florian N. and Abrazhevich, Dennis – Eindhoven University of Technology, The Netherlands
Towards a Model of Trust for E-Commerce System Design, 2000, (http://www.zurich.ibm.com/~mrs/chi2000/contributions/egger.html)
Security & Trust: Taking Care of the Human Factor, ePSO-Newsletter No.9, September 2001 (http://epso.jrc.es/newsletter/newsletter.html) [Puts forward a user-centred perspective of the problem of trust in online payments, derived from the discipline of Human-Computer Interaction (HCI)]

Einwiller S., Geissler U. and Will M. – Institute for Media and Communications Management, University of St. Gallen, Switzerland
Engendering Trust in Internet Business using Elements of Corporate Branding, 2001

Electronic Commerce Branch Industry Canada
Building Trust and Confidence in Electronic Commerce: A framework for Electronic Authentication in Canada, July 2000, (http://e-com.ic.gc.ca/english/authen/doc/framework.pdf) [Describes electronic authentication and certification services. It identifies the need to provide a co-ordinated approach, that a framework has to be established and that international dimensions must be taken into consideration]

European Parliament and the Council of the European Union

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the movement of such data

Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases

Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts

Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications network

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Jan 19th 2000

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce in the internal market

European Commission
97/489/EC Commission recommendation of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, (europa.eu.int/ISPO/ecommerce/legal/documents/recpay.zip)

Study on the implementation of Recommendation 97/489/EC – Final report 20 March 2001, (http://europa.eu.int/comm/internal_market/en/finances/payment/instrument/study.htm)

98/257/EC Communication recommendation on the principles applicable to the bodies responsible for out-of-court settlement of consumer disputes,
(http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just02_en.html

2001/310/EC Commission recommendation of 4 April 2001 on the principles for out-of-court bodies involved in the consensual resolution of consumer disputes,
(http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just12_en.pdf)

DG Internal Market, Financial Services, Retail Issues and Payment Systems, MARKT/173/2000, 12 July 2000, „Payment Card Chargeback when paying over Internet", First Sub-group meeting of the PSTDG and PSULG held on 4 July 2000, Working Document,
(http://europa.eu.int/comm/internal_market/en/ecommerce/chargeback.pdf)

Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions, on "Creating a Safer Internet Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime", eEurope 2002, COM (2000) 890 final, Brussels 26.1.2001,
(http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComm EN.html)

Communication from the Commission to the Council, the European Parliament, the European Central Bank, the Economic and Social Committee, and Europol, on "Preventing fraud and counterfeiting of non-cash means of payment", COM (2001) 11 final, on 9.2. 2001,
(http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/fraudprevent/prevfraud_en.pdf)

Proposal for a Council Framework Decision on attacks against information systems, COM (2002) 173 final, on 19.04.2002 (http://europa.eu.int/eur-lex/en/com/pdf/2002/com2002_0173en01.pdf)

Green Paper on European Union Consumer Protection, Brussels, 2.10.2001 COM (2001) 531 final,
(http://www.computerundrecht.de/docs/green_paper_on_eu_consumer_protection.pdf)

European Commission, Commissioner General Health and Consumer Protection, David Byrne
David Byrne Welcomes breakthrough in helping consumers shop online with confidence, Brussels 10 December 2001

European Commission, Director General Health and Consumer Protection, Robert J. Coleman
Communicating Risk to Consumers at the Syngenta Round Table Meeting, Brussels 17 October 2001

Address concerning Consumers and the Internet at the AIM Brand Forum 2001, Brussels 6 Nov 2001

European Commission, Joint Research Centre, IPTS
Cybercrime, Report on a JRC Workshop held at IPTS 11-12 January, 2001,
(http://www.jrc.cec.eu.int/download/press/releases/cybercrime_010212.pdf)

Gartner Group
On-line Fraud Prevention White Paper for the E-Commerce Fraud Prevention Network, March 2001,
(http://www.gartner.com/)

GBDe - Global Business Dialogue on electronic Commerce
Consumer Confidence web site, (http://consumerconfidence.gbde.org)

Gefen, David – Drexel University (Philadelphia, US) and Straub, Detmar – Georgia State University (Atlanta, US)
Managing User Trust in B2C e-Services, Sep 2000,
(http://www.lebow.drexel.edu/gefen/eServiceJournal2001.pdf) [Examines the effect of social presence on consumer trust in e-Services and the relative importance of consumer trust in comparison with the widely studied Technology Acceptance Model – TAM beliefs. The study concludes that firms that excel in instilling high degree of social presence in their websites may prosper more than those that do not]

Gpayments – Authentication and Payment Solutions
VISA 3D-Secure vs. MasterCard SPA, March 2002, (http://www.gpayments.com/pdfs/GPayments_3-D_vs_SPA_Whitepaper.pdf) [This white paper compares the standards examining them from the perspectives of cardholders, issuers, merchants and acquirers. It also compares the standards from both a general architecture and a security architecture perspective]

IDG
Web merchants stung by credit-card fraud, 11 March 1999,
(http://www.cnn.com/TECH/computing/9903/11/webfraud.idg/)

Information Security Magazine
Industry Survey, October 2001, (www.infosecuritymag.com)

Internet Fraud Complaint Center – IFCC, US
a- IFCC Internet Fraud Report (January 1, 2001 – December 31, 2001)
b- Internet Auction Fraud Report (May 2001)
c- Six Months Data Trends Report (May - November 2000)
(http://www1.ifccfbi.gov/strategy/statistics.asp)

Jarvenpaa, Sirkka L. – University of Texas, Department of Management Science and Information Systems and Tractinsky, Noam – Ben-Gurion University, Industrial Engineering and Management
Consumer Trust in an Internet Store: A Cross - Cultural Validation, December 1999
(http://www.ascusc.org/jcmc/vol5/issue2/jarvenpaa.html) [Report on a cross-cultural validation of an Internet consumer trust model. The model examines both antecedents and consequences of consumer trust in a Web merchant].

Klasen, Dirk – Bundesverband der Verbraucher-Zentralen und Verbraucherverbände, Federation of German Consumer Organisations, Germany
Creating Consumer Confidence: Current Efforts towards International Quality Criteria for E-Commerce, ePSO-Newsletter No.9, September 2001, (http://epso.jrc.es/newsletter/newsletter.html)

Knapp, Wade M. - CPS
Understanding Crime Risk Management, Protective Research Group, 2000,
(http://www.proresearchgroup.com/articles/riskmngmnt.pdf)

KPMG Forensic and Litigation Services
2001 Global e.fr@ud.survey,
(http://www.kpmg.ca/english/services/docs/fas/efraud2001.pdf)

Lang, Paul
How to beat credit card fraud, 1999, (http://scambusters.com/reports/lang.html)

Lelieveldt, Simon
New payment authentication methods for use on the Internet, ePSO-Newsletter No.8, July 2001, (http://epso.jrc.es/newsletter/newsletter.html) [Describes the three models for authentication over the Internet, which may be adopted by Visa (3D secure), Mastercard (Secure Payment Application) and Maestro, as presented during the recent Second Edinburgh Financial Cryptography Engineering Conference]

NCL – National Consumer's League, US
2001 Shopping Online Survey
On-line Auctions 2001 Survey – Summary of findings
6 Tips for Shopping Safety
(http://www.nclnet.org/shoppingonline/index.htm)

OECD – Organisation for Economic Co-operation and Development
Guidelines for Consumer Protection in the Context of Electronic Commerce, Dec 1999, (http://www.oecd.org/pdf/M00000000/M00000363.pdf)
Building trust in the Online Environment: Business to Consumer Dispute Resolution, Joint Conference of the OECD, HCOPIL, ICC, Report of the Conference, The Hage 11-12 December 2000; OECD Papers 2001 Volume 1, No.3, 19 April 2001.

Office of Consumer Affairs (OCA) of Industry Canada
Principles for Consumer Protection in Electronic Commerce – A Canadian Framework, November 1999, (http://www.cba.ca/Eng/Publications/Ecomm/principlese.pdf)

Office of Management and Budget – OMB, US
FY2001 Report to Congress on Federal Government Information Security reform, March 2002, (www.whitehouse.gov/omb)

Rich Pethia, Software Engineering Institute Carnegie Mellon University, Pittsburgh
Internet Security Trends, 2001, CERT/CC – Computer Emergency Response Team / Co-ordination Center, (www.cert.org)

Pichler, Rufus – Stanford Law School, Standford University
Trust and Reliance – Enforcement and Compliance: Enhancing Consumer Confidence in the Electronic Marketplace, May 2000, (http://lawschool.stanford.edu/library/special/rufus.thesis.pdf)

Powell, Douglas A. – University of Guelph, Guelph, Ontario
Food Safety and The Consumer – Perils of Poor Risk Communication, Powell, D.A., Can. J. An. Sci. 80(3): 393-404, 2000, (http://www.foodsafetynetwork.ca/risk/powell.html)

Resnick, Paul and Zeckhauser, Richard
Trust Among Strangers in Internet Transactions: Empirical Analysis of eBay's Reputation System, Working paper for the NBER workshop on empirical studies on e-commerce, 2001 (http://www.si.umich.edu/~presnick/papers/ebayNBER/index.html)

Resnick, Paul; Zeckhauser, Richard, et al.
Reputation Systems: Facilitating Trust in Internet Interactions, Communications of the ACM, 2000, pages 45-48, draft version (http://www.si.umich.edu/~presnick/papers/cacm00/reputations.pdf)

Schneier, Bruce – CounterPane
Liability and Security, Crypto-gram Newsletter, April 15, 2002 (http://www.counterpane.com/crypto-gram-0204.html)

Electronic Commerce: The Future of Fraud, Crypto-Gram Newsletter, Nov 15, 1998 (http://www.counterpane.com/crypto-gram-9811.html)

The process of security, Information Security Magazine, April 2000 (http://www.infosecuritymag.com/articles/april00/columns_cryptorhythms.shtml)
[Security doesn't have to be perfect. But risks do have to be manageable. The problem is, users don't understand the risks, and products alone can't solve security problems]

Secrets and Lies, Digital Security in a Networked World, 2000, ISBN 0-471-25311-1

SET - Secure Electronic Transaction Specification
Book 1: Business Description, May 31, 1997, (www.setco.org)

Spafford, Gene – Center for Education and Research in Information Assurance and Security (CERIAS), US
PKI Forum Exclusive Interview, Feb 2002, (http://pkiforum.com/books/interview_spafford.html) [Presents his view of, among others, the general security landscape; major challenges in information security; the need for advanced security solutions; security infrastructure; PKI and its difficulty with interoperability; PKI and privacy, organisational control and liability; premature deployment of PKI and its dangers; the need for key back-up and recovery by trusted third parties and the need for security skilled people in academia and in business]

Swaminathan, Vanitha – University of Massachusetts-Amherst, Isenberg School of Management; Lepowska-White – Skidmore College, Department of Management and Business and Rao, Bharat P. – Polytechnic University, Institute for Technology and Enterprise
Browsers or Buyers in Cyberspace? An Investigation of Factors Influencing Electronic Exchange, 1999, (http://www.ascusc.org/jcmc/vol5/issue2/swaminathan.htm)

Stroborn, Karsten
Online-Umfrage: So will der Kunde im Internet bezahlen. In: IIR: C@shWorld. 5. IIR-Kongress Zahlungssysteme im eBusiness, 6.-8.2.2001. Proceedings. Frankfurt am Main: IIR 2001, (http://www.iww.uni-karlsruhe.de/IZV4/) [The survey underlines the role of traditional payment methods even for experienced Internet users and savvy online-shoppers]

TACD – Trans Atlantic Consumer Dialogue
Payment Card Redress and Protections, Doc No. Ecom-23-01, May 2001, (http://www.tacd.org/cgi-bin/db.cgi?page=view&config=admin/docs.cfg&id=95)

Van Hove, Leo – Free University of Brussels, Belgium
The Payment Blues of German Internet Merchants, ePSO-Newsletter No.9, Sept 2001, (http://epso.jrc.es/newsletter/newsletter.html) [Comments a report from Berlecon Research "Kassieren im Ecommerce – eine Analyse relevanter Zahlungssysteme aus Händlersicht"]

VISA EU – Virtual VISA
Three domain Model Fact Sheet, August 2000, (http://visaeu.com/virtual_visa/presscentre/factsheets/three_domain_model.html)

Account Information Security Programme (http://www.visaeu.com/for_business/e-commerce_security/ais_programme.html)

Wahlberg, Anders Af and Sjoberg, Lennart – Center for Risk Research
Risk perception and the media, Journal of Risk Research 3(1), 31-50 (2000), (http://www.foodsafetynetwork.ca/risk/j-risk-research.pdf)

Walker, T. J.
Don't be victimized by Online Credit Card Fraud – Prevention Tips, 1999, (http://scambusters.com/reports/walker.html)

Walczuch, Rita and Seelen, Joyce – University of Maastricht & International Institute of Infonomics, The Netherlands
Psychological reasons for consumer trust in e-retailing, Project e-behaviour, 2000, (http://www.ub.unimaas.nl) [The psychological factors expected to influence trust are personality-based factors, perception-based factors, experience-based factors, knowledge-based factors and attitude. The results of a pilot conducted in the Netherlands are included in the paper]

Weber, Arnd – ITAS, Karlsruhe, Germany
Interview: Larget German Credit Card Issuer on Massive Reduction of ChargeBacks, ePSO-Newsletter No.10, November 2001, (http://epso.jrc.es/newsletter/newsletter.html)

Additional useful links

- europa.eu.int/comm/internal_market/en/ecommerce, EC DG Internal Market, Electronic Commerce
- europa.eu.int/comm/internal_market/en/finances/payment/fraud/index.htm, EC DG Internal Market, Financial Services, Payments, site on Fraud and Counterfeiting
- econfidence.jrc.it/, an EC DG Health and Consumer Protection initiative promoting information exchange and discussions about e-Confidence
- www.commerce.net, a non-profit consortium of business, government, technology and academic leaders, to jointly develop and implement e-commerce technologies and business practices world-wide
- www.couterpane.com/crypto-gram.html, monthly newsletter by Bruce Schneier
- www.diffuse.org/secguide.html, Guide to Information Security
- www.fraud.org/internet/intset.htm, US National Consumers League, Internet Fraud Watch
- www1.ifccfbi.gov/index.asp, Internet Fraud Complaint Center - IFCC, a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C).
- www.sans.org, SANS – System Administration Networking and Security Institute
- www.webcredibility.org, Web Credibility Research, with the goal to understand what leads people to believe what they find on the Web

- Consumer Interests sites:
  - www.beuc.org, BEUC - Bureau Européen des Unions des Consommateurs
  - www.consumerPrivacyGuide.org, offers tips on how to read and understand the privacy policies of on-line retailers and other web sites, co-sponsored by five consumer groups
  - www.consumer.gov/sentinel, FTC Consumer Sentinel, an international law enforcement fraud-fighting program
  - www.consumersinternational.org, Consumers International, a world-wide organisation
  - www.econsumer.gov, site for gathering cross-border e-commerce complaints and sharing consumer protection information, with participation by 15 countries and the OECD
  - www.ftc.gov/bcp/menu-internet.htm, Federal Trade Commission Consumer Protection for Internet and electronic Commerce
  - www.isalliance.org, the Internet Security Alliance, a global industry forum for information sharing and thought leadership on information security issues.
  - www.nclnet.org, US National Consumers League - NCL
  - www.scambusters.org, Internet Scambusters, The #1 publication on Internet Fraud
  - www.staysafeonline.info, the US National Cyber Security Alliance, a co-operative effort between industry and government organisations to foster awareness of cyber security through educational outreach and public awareness.
  - www.tacd.org, Transatlantic Consumer Dialogue

- Merchant Interest sites:
  - www.Antifraud.com, “The Front line of Defense for Online Commerce”
  - www.fraudforum.org, a not-for-profit organisation geared towards providing advice and support for both individuals and businesses, and in particular the SME community
  - http://www.scambusters.com/CreditCardFraud.html, strategies for merchants to reduce credit card fraud
  - www.unice.org, Union of Industrial and Employers’ Confederations of Europe