OECD Digital Economy Papers No. 64

Report on Consumer Protections for Payment Cardholders

OECD

https://dx.doi.org/10.1787/233364634144

OECD

Unclassified **DSTI/CP(2001)3/FINAL**

Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

14-Jun-2002

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE ON CONSUMER POLICY

DSTI/CP(2001)3/FINAL
Unclassified

REPORT ON CONSUMER PROTECTIONS FOR PAYMENT CARDHOLDERS

English - Or. English

JT00128255

FOREWORD

The OECD Committee on Consumer Policy (CCP) has been working for a number of years to analyse and strengthen consumer protections for holders of payment cards. Most recently this effort has included a survey of protections currently available in OECD Member countries and a roundtable on consumer protections for payment cardholders, held in Berlin, Germany, on 15 March 2001. This report summarises the results of this work, presenting the first comprehensive look at this issue by the OECD since the emergence of e-commerce over the past several years.

The report begins with a look at the use of payment cards in business to consumer e-commerce, the role of the payment card network, and the types of consumer protection issues that arise. The second part of the report discusses the laws and practices relating to consumer protection for payment cardholders in OECD Member countries. The concluding section focuses on the importance of cardholder education. As a step toward addressing the educational issue, the Committee developed a consumer education piece, "Using Payment Cards Online: Frequently Asked Questions", which is attached as an annex.

At its March 2002 meeting the CCP agreed to declassify this report under a written procedure completed on 24 May 2002. It is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

REPORT ON CONSUMER PROTECTIONS FOR PAYMENT CARDHOLDERS

Introduction

Many active Internet users remain unwilling to purchase goods or services over the Internet. Opinion surveys consistently identify consumer fears about the safety of using payment cards online as the key reason for this unwillingness. A June 2001 Gallup poll found that only 33% of global Internet users were "comfortable" providing credit card information online, and that more than eight in ten users (82%) said they were "very concerned" or "somewhat concerned" about the misuse of credit card information given out on the Internet (Jones and Carlson, 2001). Jupiter Media Metrix found consumers to be "overwhelmingly" fearful about the theft of credit card data online, with nearly 81% of US consumers afraid that their card number will be intercepted online (eMarketer, 2001). A recent National Consumers League survey concludes that the biggest consumer worry regarding online shopping continues to be the theft of credit card numbers (NCL, 2001). The Australian National Office for Information Economy (NOIE) reported that consumer misgivings regarding the safety of online financial transactions remain the number one hurdle to more active online purchasing (NOIE, 2000). As observed by the *The Economist* magazine, the most serious obstacle to global e-commerce success is "customers' terror of launching their financial details into cyberspace" (*The Economist*, 2000).

These concerns suggest that consumer protections for payment cardholders – sometimes informally referred to as "chargebacks" – have an important role to play in developing the business-to-consumer electronic marketplace. The protections currently available to cardholders vary considerably between and even within OECD Member countries. They can include anything from a consumer's ability to have billing errors corrected, to liability limits for unauthorised charges, to redress for goods not received. In some instances these protections are required as a matter of national law or regulation, but in others they are provided voluntarily through industry codes or other programmes by card issuers. In either case, they are typically implemented through the payment card networks' chargeback mechanisms (discussed further below). These payment card networks have global reach, thereby considerably reducing redress challenges for consumers shopping across national borders. When provided in a transparent and effective manner, cardholder protections increase consumer confidence in the use of payment cards for online purchases, and in the global marketplace more generally.

Over the last several years the OECD has focused on initiatives aimed at encouraging the development of fair and effective mechanisms for resolving disputes between businesses and consumers engaged in cross-border e-commerce. These efforts have included work in e-commerce consumer protection, electronic privacy and security, online alternative dispute resolution, and consumer protections for holders of payment cards – the focus of this report. The OECD *Guidelines on Consumer Protection in the Context of Electronic Commerce*, developed by the Committee on Consumer Policy (CCP) in 1999, highlight the important role of payment cardholder protections and enhanced consumer education in the development of the online global marketplace.

This document reports on a CCP survey of legal and other consumer protections for payment cardholders in OECD Member countries. It also incorporates information gained during the CCP Roundtable on Consumer Protection for Payment Cardholders held in March 2001 in Berlin, Germany. The Roundtable

brought together experts from academia, business, consumer groups and governments to discuss the issue of payment protections and what the OECD should be doing in this policy area.

The report begins with an overview of past OECD work in the field of consumer protection for payment cardholders. It then discusses the current state of affairs with regard to cross-border e-commerce, payment security and consumer confidence, and reviews the consumer protection issues arising from the use of payment cards. A synopsis of the consumer protection regimes currently in place for payment cardholders in OECD Member countries is presented in the second half of the report. The concluding section focuses on the importance of cardholder education. As a step towards addressing the educational issue, the Committee developed a consumer education piece, "Using Payment Cards Online: Frequently Asked Questions", which is attached as an annex.

The role of payment cards in cross-border business-to-consumer commerce

Background on work by the OECD

The CCP's work on protections for payment cardholders dates back to the June 1994 conference, "A Global Marketplace for Consumers". Following that event, the Committee began to assess the barriers to creating a global marketplace in which consumers and businesses could interact more freely. A significant international obstacle that emerged was the lack of mechanisms for consumer redress in such cases as fraud, delivery problems, defective goods, or billing complications. Ensuring payment protections for cardholders was quickly identified as one of a number of important ways in which consumers could have the means to seek redress in the new marketplace.

In 1996, the OECD held a "Roundtable on Consumer Redress in the Global Marketplace" in London and a follow-up meeting in Paris that focused on protections for payment cardholders. A report from that roundtable, *Consumer Redress in the Global Marketplace: Chargebacks*, included a survey of national laws on the subject and a list of main points for further discussion. Many of the discussion items identified – including differences among card companies and countries in their protections, questions about whether cardholder protections should be offered in cases of misrepresentation or non-conformance of goods, and debates over whether there should be a voluntary international code to extend guarantees to all transactions – continue to feature in policy discussions today.

The dramatic rise in e-commerce over the past six years has brought into sharper focus the role and importance of payment cardholder protections. The 1998 Ottawa Ministerial Declaration noted the exponential growth in the volume of consumer transactions on the global network and affirmed the importance of addressing issues that included dispute resolution and redress. The 1999 *Guidelines for Consumer Protection in the Context of Electronic Commerce* addressed the issue squarely: "Limitations of liability for unauthorised use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce."

A year later, payment cardholder protections were again part of the OECD agenda, this time at the December 2000 conference in The Hague, "Building Trust in the Online Environment: Business to Consumer Dispute Resolution," which focused on developments in online alternative dispute resolution.[1] Protections for payment cardholders also featured prominently within general discussion of e-commerce (and, in particular, discussions of the importance of refund and redress policies) at the March 2001 OECD workshop in Berlin on the 1999 *Guidelines*, "Consumers in the Online Marketplace: OECD Workshop on the *Guidelines* – One Year Later."[2] And, of course, cardholder protections were discussed extensively in the context of online transactions at the CCP Roundtable that immediately followed the Berlin workshop.

This report ties together the most recent strands of OECD work on payment cardholder protections and concludes with an educational section aimed at helping instil consumer confidence in the use of payment cards for shopping online.

Current state of affairs

E-commerce backdrop

Between the 1996 London Roundtable and the 2001 Berlin Roundtable, there was a dramatic increase in the volume of online business-to-consumer transactions. For example, in the United States, online shopping revenues have multiplied by a factor of 14 since 1997, reaching USD 54.2 billion in 2001 (eMarketer, 2001, see figure "Comparative Estimates: US B2C eCommerce Revenues, 2001"). In Europe, the online market was expected to reach EUR 8.5 billion in 2000, up from EUR 2.9 billion in 1999 (Internet Global, 2000). In the first half of 2001, German consumers alone ordered EUR 1.9 billion worth of goods via the Internet, according to research by the GfK Group's Web*Scope panel. And in Japan, business-to-consumer e-commerce almost tripled from 1999 to 2000, reaching USD 9.5 billion, up from only USD 3.4 billion in 1999 (Electronic Commerce Promotion Council of Japan *et al*., 2001). These figures represent annual, global growth rates of 50 to 100%.[3]

Not surprisingly, this increase has been coupled with an increase in use of payment cards online (whether debit cards, credit card, or some other type). *Internet World* magazine reported that 95% of online shoppers use payment cards to make their purchases (Bannan, 2001). According to Visa USA, the 95% figure remains current.[4]

The jump in online transactions has been accompanied by a rising number of consumer complaints with regard to Internet activities. The US Federal Trade Commission (FTC), for example, has reported a steady increase in the the percentage of Internet-related complaints it received through the Consumer Sentinel database, jumping from 11% in 1998 to 26% in 1999, 31% in 2000, and 41% in 2001. The largest complaint category in 2001 was identity theft (which includes such problems as the theft of payment card information), accounting for 42% of the 204 000 complaints entered into Consumer Sentinel (Federal Trade Commission, 2002). A representative of Industry Canada noted at the December 2000 Hague conference that their data showed the most common e-commerce complaints include non-delivery of goods, length of time for delivery, non-disclosure of charges/costs, product attributes and retail versus online pricing (Girouard, 2000).

Given these complaints, it is interesting to note that an international Internet sweep by the International Marketing Supervision Network (IMSN) found that only about half the Web sites worldwide provide information related to redress, such as policies on returns, exchanges and refunds.[5] When coupled with the rising number of complaints, this finding highlights the importance of payment cardholder protections to increasing confidence in the online marketplace.

Indeed, with the boom in online commerce and the rise in consumer complaints, the number of chargebacks faced by merchants for e-commerce transactions has grown. There has been a greater incidence of chargebacks for e-commerce transactions than for any other type of commerce. For example, VISA USA reported that in 1999, e-commerce merchants faced chargebacks at a rate eight times greater than that faced by merchants overall. Even as compared with other types of distance selling (which include any situation when the card is not present with the merchant for the transaction) e-commerce-related chargebacks are high – approximately 38% higher than the whole pool of distance sales.

Early indications suggest that unauthorised use of card information may be a serious problem and account for a significant proportion of chargebacks in e-commerce transactions. This problem has received

significant press attention. In many cases, cardholders are not held liable for these charges. Typically, merchants bear the brunt of fraudulent use, both in terms of higher transaction costs, and loss of payment from resulting chargebacks. According to a report by Meridien Research, in 2000, online payment fraud cost merchants USD 1.6 billion worldwide (Wolverton, 2001). Meridien estimates that that figure will rise to USD 15.5 billion in 2005. Fraud rates for cyber merchants are 30 times higher than those for traditional bricks-and-mortar merchants (Celent Communications, 2000). Some estimates put the costs of fraud for online merchants during the 2000 holiday season at USD 300 million, 3% of e-commerce sales (Celent Communications, 2000).

Efforts to find solutions

Policy makers at the national and international levels are taking these concerns seriously. A number of initiatives aimed at combating payment card fraud, improving the security of online transactions, and boosting consumer protections for cardholders were presented to, and by, participants at the Berlin Roundtable. They noted that although the protections implemented through the chargebackprocess should not be considered a form of alternative dispute resolution (ADR), they do provide consumers with important redress mechanisms to assist in combating either truly unscrupulous practices or simply technical mistakes – especially in the e-commerce arena. These protections are particularly useful in cross-border transactions, where they can permit consumers to gain redress without having to address such complicated issues as jurisdiction and applicable law.

In general, participants at the Roundtable applauded efforts by businesses, consumer groups and governments to expand protections for consumers and increase consumer confidence in e-commerce by providing better safeguards for payment card transactions online. It is an issue in which there is strong incentive for business, card issuers and consumers to strive for progress.

In fact, while laws and regulations do play a critical role in providing protections (and are discussed below in detail), many of the advances in this area have come as a result of private sector-led technological developments and voluntary moves to boost protections – often motivated by the competition for customers. Card networks and their issuers have taken steps to address concerns voiced by all stakeholders by working to boost the privacy and security of electronic transactions. For example, the common use of Secure Sockets Layer (SSL) technology provides the benefit of encryption to the transfer of transaction details. Visa has recently rolled out a new service to its US customers that allows consumers to add personal passwords to existing Visa cards ("Verified by Visa"[6]). Recently, some issuers have also introduced "disposable" card numbers that can only be used once. In addition, others use smart cards that embed card data in a microchip. Simpler mechanisms include the use of personal identification (PIN) numbers.

Merchants can also take steps to prevent frauds. Software solutions include applications that look for patterns of questionable behaviour or other indicators of irregularity. Address verification services (AVS), conducted by payment processors, help ensure that the cardholder's billing address matches the shipping address.[7] Further, in the United States under a new Californian law, merchants will have to install terminals that only print the last five numbers of a credit card on the receipt (Breitkopf, 2000). However, the hacking of payment card information often comes from security problems on the storage side, not in the act of transmission. Therefore, merchants also can take both managerial and technical steps to increase the electronic and physical security of their stored payment card data.

More comprehensive solutions may require greater technological complexity. These include digital certificates, digital signatures, and the development of "digital cash" so that card information would not need to be revealed at every purchase. The emerging field of biometrics, which uses personal, biological

data for identification, also offers potential tools for increasing security, but may require significant investment to be successfully implemented and may also raise privacy concerns depending on how used. In addition, card-swipe enabled keyboards may be able to help authenticate payment card users.

In the meantime, the frequent reports of fraud appear to have a significant effect on consumer confidence and, thus, may be presenting a significant handicap to the growth of e-commerce. Can conclusions be drawn as to whether these effects appear more pronounced in countries for which the consumer protections typically afforded cardholders – either voluntarily or by law – are less visible and less transparent? One point that emerged from the Berlin Roundtable was that greater attention to the challenge of educating consumers about protections for payment cardholders and the safe use of payment cards online could serve to boost consumer confidence.

Primer on dispute resolution via payment card network

Kinds of payment cards

While there are four main types of payment cards, as described below, some cards may support several functions at the same time.

"Pay later" cards

- *Charge cards* - where the total amount incurred with the card in a billing period must be settled at once by a date agreed upon in the contract.
- *Credit cards* - where (part of) the amount due may be rescheduled at the end of the fixed period and paid by instalments. The credit card gives access to a line of credit.

"Pay now" cards

- *Debit card* - where the amount due is deducted from the cardholder's account almost immediately, without further authorisation from the cardholder.

"Pay before" cards

- *Stored value card / pre-paid card / e-purse* - a card on which value can be stored (electronically, on a microchip, etc.). The value diminishes as the card is used to make payments. Some of these cards can be reloaded to replenish the value stored on them.

Whether a card falls into one category or another is not always apparent from the card itself. Often it is necessary to consult the contract between the issuer of the card and the holder of the card in order to identify the appropriate classification. For example, the contract determines when and how the cardholder should pay the amounts incurred. There are considerable variations among OECD Member countries in this respect. While in some countries the most common cards typically have a credit line attached to them, in other countries the most common cards are debit cards or charge cards. In the case of pay now or pay later cards, however, the core characteristics of the chargebacks system described below largely remain the same.

Parties to the payment card system

There are four central parties to the card systems operated by international payment card companies: card issuers, cardholders, acquirers, and merchants (Figure 1). The relationships among these parties are

governed by a complex mix of national legislation, industry codes, card network operating regulations, individual contracts, and company policy and practice.

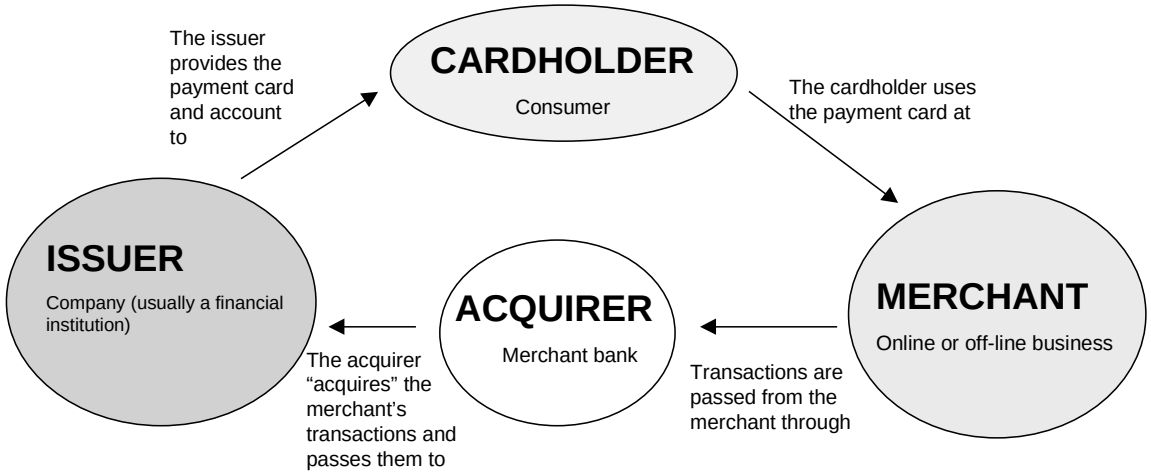
1. *Issuer*: The card issuer is the company, typically a financial institution, that provides the card (and account) to the consumer/cardholder.

2. *Cardholder*: The consumer in this system is the cardholder. In order to participate, the cardholder will have entered into a contract, the "cardholder agreement", which will serve as the primary instrument governing the relationship with a card issuer.

3. *Acquirer*: Sometimes referred to as the merchant bank, this financial institution "acquires" the transactions from the merchant and passes them on to the card issuer (via the card network). The operating regulations of card networks govern the relationships between acquirers and issuers.

4. *Merchant:* In order to accept payments via a payment card, merchants must establish a relationship with an acquirer. The contracts governing these relationships impose an obligation on the merchant to accept deductions for most transactions that are charged back to the acquirer through the system.

Figure 1. Parties to the payment card system



Source: OECD Secretariat, 2002.

The chargeback: definition and procedure

The term "chargeback" is used by the payment card industry to refer to the process by which an issuer returns a financial obligation to the acquirer. As such, chargebacks relate to the rights and obligations between financial institutions (issuers and acquirers), and only impact cardholders and merchants indirectly. However, the term is frequently used less formally to refer to the process through which cardholders obtain redress and correct errors through the card issuer. This may be due, in part, to the fact that chargeback rules assist issuers in meeting their legal obligations to cardholders under various consumer protection laws and regulations.

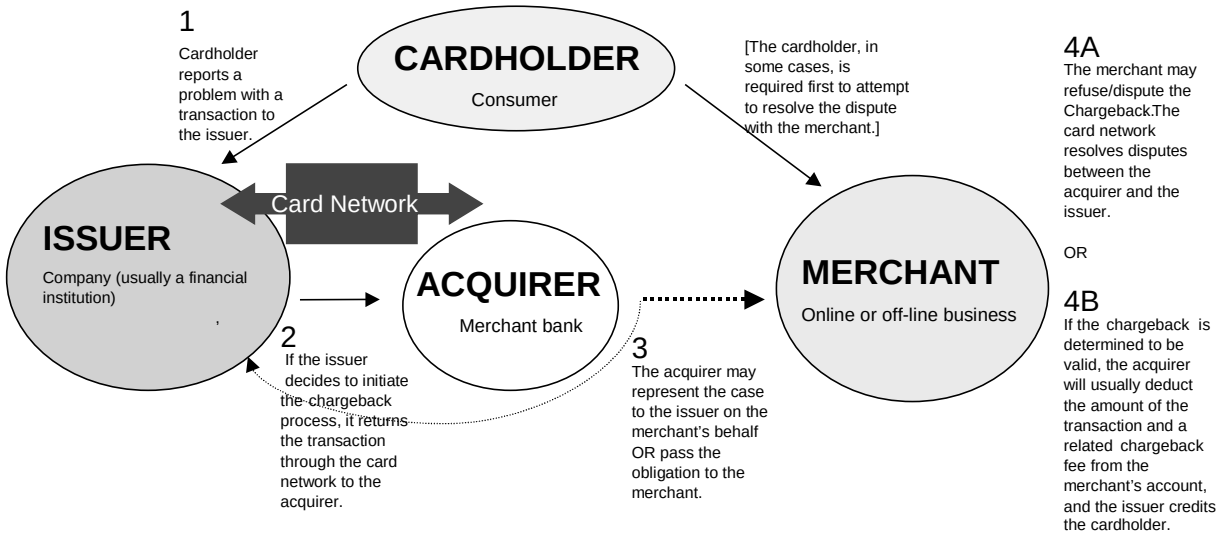
The chargeback process is governed by the operating regulations of the specific card network and national laws. Chargeback rules specify the timeframes for the dispute, the requirements to qualify as a dispute, and the remedies for the dispute. The process may function differently for different networks, different types of cards, and different types of problems or complaints. Nevertheless, common features can be identified.

Typically, the process is initiated by notice from the cardholder to the issuer that there is a problem with a transaction. Cardholder agreements and national laws often specify a notice period during which a claim must be received and sometimes require that the notice be in writing. As indicated above the cardholder is, in some cases, required first to attempt to resolve the dispute with the merchant.

Upon receipt of the cardholder notice, the issuer then analyses the complaint, and may conduct an investigation. For example, the issuer may order a copy of the sales draft. Depending on the results of the analysis/investigation, the issuer may elect to initiate the chargeback process by returning the transaction through the card network to the acquiring bank.

The acquirer may then represent the case to the issuer on the merchant's behalf or pass the obligation on to the merchant. The merchant may attempt to refuse/dispute the chargeback. Ultimately, the card network will resolve disputes between the issuer and acquirer. If the chargeback is determined to be valid, the acquirer will usually deduct the amount of the transaction and a related chargeback fee from the merchant's account, and the issuer will credit the cardholder's account. See Figure 2.

Figure 2. The chargeback process



Source: OECD Secretariat, 2002.

In principle, the chargeback process is available for each of the categories of disputes identified below ("I didn't do it", "I didn't receive it", and "I don't want it"). Whether the card issuer is willing, or obliged, to initiate the chargeback process on behalf of a cardholder is another matter. The interaction between national legislation, industry codes, card network policies, and issuer practice will shape the circumstances under which the issuer will attempt to use the chargeback mechanism to resolve a cardholder complaint. In the absence of legal, contractual, or card network obligations, the decision to initiate the chargeback process is left to the discretion of the issuer. For certain types of claims, the issuer may decide to reimburse the cardholder without actually initiating the chargeback process and without recovering the funds from the acquirer/merchant.

Consumer protection issues arising from the use of payment cards

The use of payment cards, and consequently, the chargeback system (when seeking redress) raises a number of consumer protection issues. The primary types of problems that arise from the use of payment cards can be divided into three groups: "I didn't do it" (unauthorised transactions), "I didn't receive it", and "I don't want it". In terms of using the chargeback system, there are important issues for consumers regarding the time limits associated with cardholder complaints, the transparency of the process, the burden of proof consumers must bear, the degree to which consumer carelessness can factor into the process, and the efforts the cardholder must make to resolve a problem with a merchant.

Primary types of consumer problems

i) *"I didn't do it" (Unauthorised transactions)* - includes cases where a transaction has been made and a corresponding amount is charged to the cardholder's account without his or her authorisation.

The transaction may be the result of fraud (fraudulent use), or a processing error. Fraud occurs where a payment card and/or a card number and/or a PIN number are used by an unauthorised person. In a face-to-face transaction, for example, fraudulent use may imply the use of a false signature. Processing errors occur where an undue amount (or an extra amount) is charged to the cardholder's account as a result of a technical fault or a human error in the processing of the transaction either by the merchant, the issuer or the acquirer.

These types of complaints are among the most common received by card issuers, especially in the online arena, and can sometimes result from confusion over e-commerce transactions. Consumers can mistakenly repeat purchases online (and therefore are double-billed) or may not recognise the location of a billing company from an online purchase (and therefore believe that a fraudulent charge has been added to their bill).

ii) "*I didn't receive it"* - covers cases in which the cardholder has been charged for his/her purchase but has not received the goods after a reasonable time. It may also include cases where the goods received do not match the description of what was ordered (*e.g.* a different item is delivered), and cases where the merchant goes bankrupt.

iii) "*I don't want it"* - in cases of distance selling (mail order, telephone order or online purchases), "I don't want it" may cover a range of cases including:

- Where the cardholder claims that the good received does not match the quality to be reasonably expected according to the offer (non-conforming goods).

- Where the cardholder has a right of withdrawal from a contract and that right is not matched by a corresponding obligation on the merchant to not charge him/her before the cooling off period ends, or to return the funds if right of withdrawal is exercised.

- Where the goods (or service) received are not fit for the purpose for which they were purchased.

This is often the most difficult category of complaint to address because "I don't want it" complaints can involve a fair amount of subjectivity on the part of the consumer or the merchant.

Other issues

There are also consumer protection issues implicated by the process through which cardholders raise disputes with their issuer. Some are listed below.

Time limits

Even in the most liberal chargeback system, there are usually some practices that may make it difficult for consumers to obtain redress. One of the most common is the placement of time limits on the period in which consumers must act to provide notice to the issuer. These time limits may vary from country to country or company to company. Further, within companies, they may vary again depending on whether transactions were domestic or international. They can also vary depending on the circumstance. A complaint regarding a billing item may be filed within 180 days, for instance, while a report of a lost or stolen card may require immediate notification to the issuing company in some countries.

However, time limits could also work to aid the consumer if placed on the issuing company. For example, in some countries these limits can set a defined time period in which a company must investigate and resolve a dispute.

In general, there are questions as to what comprise "reasonable" time limits both for consumers in filing complaints and companies in investigating and resolving disputes. There are similar questions as to what constitutes a "reasonable" effort to solve the dispute directly with the merchant.

Process transparency

There are also questions about the amount of transparency in the chargeback process. It is a complicated system, with varying rules depending on location and the circumstances of a complaint. For consumers to gain the most benefit, they must be able to make informed choices. The same holds true for merchants. There must at least be a significant level of transparency such that all parties and stakeholders can understand the process. Whether or not that level of transparency is now in place is debatable.

Looking ahead, the future may bring new transparency issues to the area of payment card protections. It is increasingly difficult to distinguish the functions of cheques, debit cards, and credit cards. With technological innovations allowing multiple card functions to reside in the same cards and facilitating the development of new forms of payment cards, these new types of cards may not fit cleanly into the old legal categories governing payment card protections. As a result, it may become more difficult for consumers and businesses to know exactly what their rights and responsibilities are in particular cases, and it may be necessary to review and update existing consumer law.

Burden of proof

Other issues for consideration relate to the amount of proof a consumer must provide to justify a request that a charge be nullified. One advantage for consumers in many chargeback systems is that they may minimise burdensome negotiations with merchants over disputes; leaving the card issuer or acquirer usually bear that burden (although in some circumstances the consumer may need to make a preliminary effort at direct negotiation). Often, it is also presumed that the consumer is correct unless proven wrong by the merchant.

However, many questions remain about how the frequency with which consumers benefit from these advantages. For example, how much proof must the consumer demonstrate for a chargeback process to be initiated? Must the proof come from the consumer, or should the card issuer automatically assume that the consumer is correct and instead demand proof from the merchant that it is not to blame? How much proof is necessary from the merchant to show that it, in fact, complied with its obligations in the transaction?

Carelessness

Some chargeback systems make distinctions between erroneous or fraudulent charges accrued as a result of carelessness by the consumer and those accrued through no fault of the consumer. In these systems, the level of protection afforded may differ depending on the extent to which the consumer was careless. These types of systems then raise similar questions to those under the "burden of proof" category: How careful must a consumer be to have full protection? How must the consumer prove this? Or, on the contrary, how much proof must an issuer provide to show that a consumer was careless, in order to avoid liability?

Direct resolution with merchant

Another typical issue for consideration relates to what efforts a cardholder is required to make to attempt to resolve the dispute with the merchant before approaching the card issuer to seek redress. Included here is the extent to which the cardholder must provide written documentation to prove that the necessary efforts were made.

Consumer protection regimes for payment cardholders

There are varied approaches to consumer protection for payment cardholders in OECD Member countries. These levels of safeguards include:

- Legal or regulatory regimes.
- Protections mandated by industry practice.
- Protections provided through individual issuer initiatives.
- Recommendations by international organisations

The first section below will discuss the various legal regimes implemented in Member countries, while the sections that follow will discuss other, less formal protections – that is, those recommended by international organisations or mandated by industry practice and those provided through issuer initiatives. Many of these schemes offer layers of protection that overlap or enhance the protections offered in particular countries that also have legal or regulatory regimes in place.

Protections mandated by legal or regulatory regimes

Overview

Not all OECD Member countries have legal or regulatory regimes covering consumer protections for payment cardholders. Further, there are great differences among those that do have these regimes. While many Member countries, for example, have specific provisions with regard to unauthorised charges and

processing errors, not as many have specific provisions addressing non-delivery or non-conforming goods and services. Even fewer Member countries have specific provisions that discuss consumer satisfaction issues. There also are differences among nations with regard to the types of problems that are addressed by specific legal provisions, and those which are either left to guidelines, industry practice, or up to consumers to work out with merchants on their own. Among the differences of particular relevance to e-commerce are whether or not the regimes cover all payment cards and how the regimes treat domestic versus international transactions.

Some of the important issues for online transactions arising from a comparison of the existing legal and regulatory regimes in OECD Member countries are discussed below. The discussion focuses on provisions related to unauthorised use, non-delivery, non-conforming goods and services, protections for different types of payment cards, and applicability to cross-border transactions.

Unauthorised use

Several OECD Member countries have specific legal or regulatory provisions dealing with unauthorised charges to payment cards. Those Member countries with these provisions include Belgium, Denmark, Finland, Greece, Hungary, Korea, Mexico, Norway, Sweden, the United Kingdom and the United States. In addition, while Canada has no specific national provisions in place, provincial legislation is in the process of being prepared.

Where there are specific legal or regulatory provisions, levels of protection guaranteed by them may vary. A key determinant in countries such as Belgium, Denmark, Korea, Norway and Sweden appears to be whether there was negligence on the part of the consumer. In Belgium, for instance, there are different ceilings of liability that take into account such factors as whether negligence, or extreme negligence, played a role, and whether fraud was committed before and/or after notification. In Sweden, consumers are only liable if the card was given to a third party, if it was lost negligently, or if the cardholder fails to notify the issuer immediately. In Korea, an issuer can contract out of liability in the event of a “serious mistake” by a cardholder. By contrast, in the United States, the maximum statutory liability for credit cardholders is USD 50 for unauthorised use.

Non-delivery

Few OECD Member countries report having specific legal or regulatory provisions protecting cardholders in cases of non-delivery of goods or non-performance of services. Among those that do are Finland, Greece, Japan, Korea, Norway, the United Kingdom, and the United States. In countries without such specific provisions, some rely on other laws or are preparing legislation in this area.

The details of the provisions differ among the countries with specific provisions already in place, although the focus in all is providing consumers with some ability to avoid liability for charges incurred if goods are not delivered in a timely manner. In Japan, credit cardholders can raise claims against the issuer in some cases of non-delivery, and in the United States credit cardholders can delay payment of disputed amounts or have such funds provisionally restored while the dispute is being resolved. Meanwhile, in Korea, both credit and debit cardholders can refuse payment if goods are not delivered.

Legal and regulatory provisions also often address issues of connected liability. In Finland, for example, the Consumer Credit Act includes provisions for connecting the liability of the merchant to the card issuer. In the United Kingdom, for items between GPB 100 and GPB 30 000, both the creditor and the supplier are liable in the event of breach of contract or misrepresentation.

Non-conforming goods and services

Member countries with specific provisions on non-conforming goods and services include Finland, Greece, Japan, Korea, Norway, the United Kingdom, and the United States. For example, Finnish law in this area provides protections equal to those for non-delivery; that is, there is connected liability for the merchant and the credit issuer. Korean laws provide for rights of withdrawal in some circumstances, although, in practice, cardholders usually seek resolution of disputes through mediation by the card issuer.

Only Denmark, Italy and the United Kingdom report having specific provisions dealing with consumer satisfaction issues. In the United Kingdom, for example, for items between GPB 100 and GPB 30 000, both the merchant and the issuer are liable in the event of breach of contract or misrepresentation. This, however, only applies to credit cards. In Italy, the legal protection is afforded solely for non-face-to-face contracts.

Different protections for different types of payment cards

One key question as new payment methods, such as prepaid cards, evolve is whether current legal and regulatory regimes cover all payment cards and not only the more traditional credit and debit cards. These new cards may eventually be a major component of the online business-to-consumer marketplace.

New legislation in Denmark provides an example of law that covers *all* payment cards. The legislation, passed in July 2000, applies to all kinds of electronic payments that are offered or available for use in Denmark. The law provides for protections in such areas as processing errors, transparency, options of payment methods, fraudulent use, and confidentiality/data protection. Under the new law, consumers would be liable for unauthorised charges in some cases where they were irresponsible, and up to variable limits. For non-delivery problems, relevant protections are provided in the Consumer Ombudsman Guidelines; however, there are no specific legal provisions because that issue is considered a part of the purchase commitment between a seller and buyer/cardholder. The same rationale holds true for the lack of specific legal protection in the case of defective goods or services.

In the United States, long-standing legislation provides significant protections to cardholders of credit cards. However, the laws provide less protection for holders of debit cards, and it is unclear how the laws apply to newly emerging cards. In general, holders of credit cards are well protected. US law contains specific provisions with regard to unauthorised charges, processing errors, non-delivery, non-conforming goods/services, and notice. For distance sales, the usual protections apply as to foreign merchants, and claims of unauthorised use for “card-not-present” transactions are usually successful for both credit and debit cardholders. However, debit cardholders’ protections are weaker in other areas. Debit cardholders face, among other disadvantages, variable liability limits for unauthorised use and a lack of specific protection in the cases of non-delivery and non-conforming goods/services. Therefore, while both credit and debit cardholders enjoy significant consumer protections in the United States, there are real differences in the levels of protection afforded to holders of the different cards.

These card-specific rules are not limited to the United States. Austria, Canada, Finland, Greece and the United Kingdom are among the other Member countries that also differentiate protection levels based on whether a consumer is using a credit or a debit card. An issue for future examination is how these legal and regulatory regimes will apply to other payment systems once they come into more widespread use by consumers, especially in their online purchases. Consumers may wish to use other systems to avoid the disclosure of their credit card information. However, in doing so, they may relinquish consumer protections unless these laws and regulatory regimes apply to the new payment systems. Already the

United Kingdom, among other European nations, is amending some of its laws under the Distance Selling Directive such that at least some of the provisions will apply to all types of payment cards.

Applicability to cross-border transactions

In addition to differences in the treatment of payment cards, current legal and regulatory regimes sometimes also differentiate between domestic and cross-border transactions. In an era where e-commerce is breaking down barriers between national jurisdictions, this issue can be especially important. A lack of resolution could leave consumers either confused as to when protections apply in one case or over-confident in their protections in another.

The United Kingdom provides an example of a Member country where there may be more comprehensive protections for domestic transactions than for cross-border transactions. There are questions as to whether the Consumer Credit Act's section on liability in cases of breach of contract or misrepresentation applies to overseas transactions. However, the new Distance Selling Regulations (implementing EU Directive 97/7/EC) provide that if fraudulent use is made of a consumer's credit, debit or stored-value card for distance selling purposes, the consumer is entitled to cancel payment and to be reimbursed in full by the issuer. By contrast, in the United States cardholders doing business with merchants outside the United States are covered by the same federal legal protections as those afforded them when trading with merchants within the United States.

Protections mandated by industry practice

In addition to laws and regulations, important protections are also provided by industry practice through such means as industry codes, card network requirements and individual issuer initiatives.

Industry codes

In a number of countries the card industry has implemented self-regulatory codes that contain provisions relevant to card-related protections and the rights and responsibilities of the parties to the card system. They are developed by industry, often in partnership with governments and consumer representatives. Compliance with such codes can be voluntary or obligatory, either by an industry association or government body.

For example, the New Zealand Bankers' Association has issued a Code of Banking Practice for its member banks. The Code is a self-regulatory regime, and the Banking Ombudsman monitors compliance with it. The Code clarifies the obligations of bankers and consumers in respect of the loss or theft of cards. Consumers' liability for unauthorised transactions on a lost or stolen card differs depending on whether they have acted fraudulently or negligently or have contributed to the loss.

Similarly, the Australian Banking Industry Ombudsman is an industry-based scheme that provides individuals and small businesses with an external means of investigating and resolving their complaints about banking services. Australia also has an Electronic Funds Transfer Code of Conduct (EFT Code), developed by a working group of government, industry and consumer representatives that has been subscribed to by most financial institutions offering retail electronic funds transfer services in Australia. The recently revised code covers all forms of electronic funds transfers, including ATM and EFTPOS transactions, telephone and internet banking, all credit card transactions (other than those intended to be authenticated by a manual signature), and stored value products such as smart cards, pre-paid telephone cards and digital cash. The code delivers protection by detailing the allocation of liability for unauthorised

transactions and system or equipment malfunction. It clearly explains when the institution is liable, when the consumer is liable, and when and how liability is split between consumers and the institution. Under the revised code, institutions will have to meet a higher standard of proof before a consumer can be held liable for an unauthorised transaction. In addition, the code details: the disclosure consumers must receive before they first use a new form of electronic banking; the information consumers must receive on receipts; protection of a consumer's privacy; that, when the customer agrees, electronic communications rather than paper ones are allowed; and complaints investigation and dispute resolution processes. Compliance with the EFT Code is monitored by Australian regulatory authorities and by banking industry self-regulation.

In Italy, card-issuing banks have voluntarily established an ombudsman panel for settling low-value disputes. Consumers can apply to the ombudsman after dealing with a particular bank's own complaints department, but only if the consumers have not already filed a claim in court.

Card network requirements

The major card networks impose obligations on their issuers to provide protections that may exceed those required by national laws. For example, many credit and debit card issuers promise not to hold consumers liable for unauthorised charges, even where the law only limits liability to USD 50 or more.[8] Such measures can provide important benefits to cardholders. Reponses from the Member countries focused primarily on the three largest card networks: Visa, MasterCard, and American Express. Each of these networks suggests that issuers of its cards abide by a number of policies aimed at protecting cardholders. Policies instituted by the card networks can be particularly useful because they can standardise protective measures across national borders (although they can also operate domestically). However, where they are optional, their use is left to the discretion of the individual issuer.

These initiatives are particularly focused on the problems of unauthorised use. For example, American Express promotes an online guarantee to assure its cardholders that they will not be held responsible for unauthorised charges online.[9] Visa USA advertises a "zero liability" policy for US cardholders, which promises protection against liability for certain unauthorised credit or debit charges.[10] MasterCard also advertises a "zero liability" policy for certain unauthorised uses of US-issued credit and debit cards, provided that the holder: *(i)* has an account in good standing; *(ii)* has exercised reasonable care in safeguarding the account; and *(iii)* has not reported two or more unauthorised events in the previous 12 months.[11] Visa International has recently put into effect a global policy that requires issuers to implement the chargeback process for certain kinds of complaints.

American Express reports that some card issuers will accept notice via telephone and electronic mail even though written notice is required to take advantage of legal protections. In addition, American Express has implemented a programme through which US cardholder disputes regarding charges for electronically delivered goods or services will result in an immediate chargeback. Where the goods were to be delivered physically, and the cardholder alleges that the goods were not received, the merchant will be charged back unless the goods were shipped to the cardholder's billing address, and signed for by the cardholder or an authorised representative.[12]

Card networks also are often active in promoting other, related types of online consumer protections. Visa, for example, is involved in such efforts as address verification, merchant security requirements, smart card chips, Website disclosure requirements, partnerships on seal programmes and chargebacks monitoring and detecting problem merchants.

Protections provided by issuer initiatives

In some cases, individual issuers supplement the requirements imposed by the card networks to provide additional protections for consumers. For example, some US-based issuers opted to go to the zero-liability policy for Internet purchases prior to being required to do so by the payment card networks.[13] Some of these protections are marketed specifically to allay fears of online shopping, providing protections like "purchase insurance" and "extended warranty."[14] Still others offer "$0 fraud liability," "purchase replacement protection," and a guarantee that "you won't get stuck with unsatisfactory e-purchases."[15] Issuers in various other Member countries provide similar reassurances. For example, in Australia some issuers provide protections like "online security guarantee" [16] or "100% shopping guarantee"[17].

Protections recommended by international organisations

Given the growing discussion of international payment systems for the electronic marketplace, a number of international organisations have begun to address the issue of consumer protections for payment cardholders. The OECD and the European Commission have been among the most prominent organisations in this field. Both have issued a series of recommended consumer protections for e-commerce, which include protections related to payments.

OECD

The 1999 OECD *Guidelines for Consumer Protection in the Context of Electronic Commerce* included an endorsement of the use and development of chargeback mechanisms in the field of e-commerce, especially for unauthorised and fraudulent payments. The *Guidelines* represent international consensus on the "core characteristics" for consumer protection in business-to-consumer, e-commerce transactions and were designed to ensure that consumer protection is technology neutral – that consumers are no less protected when buying online than they are when buying in a physical store or from a catalogue. In this way, the existence of chargeback mechanisms can be considered one of these core characteristics under the *Guidelines*.

The *Guidelines'* section on chargeback mechanisms provides that "[L]imitations of liability for unauthorised or fraudulent use of payment systems, and chargeback mechanisms offer powerful tools to enhance consumer confidence and their development and use should be encouraged in the context of electronic commerce."

As noted earlier, the message of this section of the *Guidelines* was echoed and highlighted by participants at the March 2001 Berlin Workshop held to discuss Member country efforts at implementation of the *Guidelines* and also at the related Roundtable on Consumer Protections for Payment Cardholders.

European Commission

There is no specific European Community consumer protection legislation that deals directly with the issue of consumer protections for payment cardholders. Some directives or other initiatives do, however, contain relevant provisions.[18]

Commission Recommendation 97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, addresses a number of issues that are relevant in the context of the contractual relationship between these two parties. Such issues include

information obligations relating to the terms and conditions of use of electronic payment instruments and the general obligations and liabilities of both parties.

With regard to losses sustained due to the loss or theft of the electronic payment instrument, the European Commission recommends that the consumer's liability should be limited in the following ways:

- Up to the notification of the loss or theft, his/her liability should not exceed EUR 150, except where he/she has acted with extreme negligence or fraudulently.
- After notification the consumer should no longer be liable for any losses, except where he/she has acted fraudulently.
- Where the payment has taken place without the physical presentation or electronic identification of the instrument itself, the consumer should not be liable for any losses.

To balance this limitation of liability, the consumer must respect his obligation to take all reasonable steps to keep his electronic payment instrument safe (including the means which enable it to be used, such as the PIN code), and must notify the issuer after becoming aware of:

- The loss or theft of the electronic payment instrument.
- The recording on his/her account of any unauthorised transaction.
- Any error or other irregularity in the maintaining of his account by the issuer.

In addition, the Commission launched a three-year Fraud Prevention Action Plan designed to crack down on payment card fraud in February 2001, and issued a Communication to the Council addressing cross-border redress, including chargebacks.[19]

The importance of cardholder education

The subject of international payment cardholder protections is not new to the CCP. However, with the explosion of e-commerce and its dependence on the use of payment cards, the environment in which these protections exist has changed dramatically over the past several years. It is likely to continue to change with the advent of new forms of electronic payment and increases in online business-to-consumer transactions.

One concern that emerged from the CCP's recent work is that consumers remain under-informed about the protections available for payment cardholders. While it is clear that protections available offer greater potential for building confidence, it is equally clear that achieving that potential requires that consumers know what protections are available and how to take advantage of them. In a few instances, the legal protections mandating cardholder protections include companion provisions designed to ensure that consumers are aware of the protections. In most countries, however, there is no legal obligation on card issuers to inform consumers about the availability of the protections that are required by law. Consumers International surveyed the actual information provided by issuers to cardholders through cardholder agreements or billing statements in a number of OECD Member countries. The results of this survey included a finding that the information provided to cardholders varied from country to country and that card companies do not consistently inform consumers about payment card dispute rights unless legally required to do so (CI, 2002).

Increasingly the major payment card networks have taken to publicising the protections provided to cardholders as a way to build brand loyalty and increase card usage. In some circumstances individual card issuers have undertaken similar initiatives.

On the whole, however, it appears that consumers do not have a good understanding of the protections available to them. For example, a survey by the National Consumer League found that 59% of consumers "mistakenly believe that it is safer to pay for an online purchase with a check or money order than with a credit cards" (NCL, 2001). Recognising the importance of this challenge, the CCP has undertaken its own educational initiative. Attached as an annex is a consumer education piece entitled "Using Payment Cards Online: Frequently Asked Questions (FAQs)". The FAQs will also be available on the consumer policy section of the OECD Web site. The Committee invites stakeholders to use these FAQs to further develop education material in languages and formats tailored to effectively communicate this message to consumers in OECD countries.

Conclusion

It is hoped that this report will assist policy makers in further exploring issues surrounding the role of payment cardholder protections in global e-commerce. Certainly, many policy challenges remain for discussion among businesses, consumer groups and governments. The CCP will continue to monitor developments on this topic as part of its ongoing work on e-commerce consumer protection. As recognised in the *Guidelines* and again at the Berlin Workshop and Roundtable in March 2001, safeguards for payment cardholders can serve an important role in addressing consumer fears about shopping online. They are likely to maintain this important role at least as long as entry in the online marketplace remains so closely linked to the use of payment cards.

REFERENCES

Australian National Office for Information Economy (NOIE) (2000), "The Phantom Menace: Setting the Record Straight About Online Credit Card Fraud for Consumers", 25 October, http://www.noie.gov.au/publications/NOIE/consumer/creditcardfraud.pdf.

Bannan, Karen J. (2001), "A Hundred Ways to Pay Online: Retailers Begin to Evaluate Alternatives to Credit Cards", *Internet World* Magazine, 15 February, http://www.internetworld.com/magazine.php?inc=021501/02.15.01internettech1.html

Breitkopf, David (2000), "States' Answer to Card Fraud: Clip Digits from Receipts", American Banker, 28 December, p.11.

Celent Communications (2000), "Online Payment Fraud: The Grinch who Stole eChristmas?", as reported by American Banker, 28 December, http://www.celent.com/PressReleases/20001218/ OnlineFraud.htm.

Consumers International (2002), "Payment Card Redress Disclosures: An international survey", http://www.consumersinternational.org.

The Economist (2000), "Making Online Payments More Secure", 26 October, p. 107.

Electronic Commerce Promotion Council of Japan (ECOM), the Ministry of Economy, Trade and Industry (METI), and Accenture (2001), "Summary of Market Research on Electronic Commerce 2000", January, http://www.ecom.or.jp/ecom_e/press/referential%20material%20final.pdf.

eMarketer (2001), *eCommerce: B2C and Demographics*, September, http://www.emarketer.com/ereports/ecommerce_b2c/welcome.html and as reported by *Newstream*, "E-Commerce Revenue to Reach $156B by 2005 – New eMarketer Report Reveals Online Shipping Continues to Grow, Despite Downturn in US Economy", September, http://www.fashionwindows.com/visualprofiles/2001/ emarket.asp.

Federal Trade Commission (2002), "Identity Theft Heads the FTC's Top 10 Consumer Fraud Complaints of 2001", 23 January, http://www.ftc.gov/opa/2002/01/idtheft.htm.

Girouard, Marcie (2000), "The [Industry Canada] Competition Bureau Experience", presentation at the OECD, HCPIL, ICC Conference on *Building Trust in the Online Environment: Business-to-Consumer Dispute Resolution*, 11-12 December 2000, The Hague, Netherlands, see Girouard presentation under Session 2, http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-44-1-no-20-1521-0,FF.html.

Internet Global (2000), Goldman Sachs report, 6 October, p. 598.

Jones, Jeffrey M. and Carlson, Darren K. (2001), "Majority of E-mail Users Express Concern about Internet Privacy", *Gallup News Service*, 28 June, http://www.gallup.com/poll/releases/pr010628.asp.

NCL (2001), National Consumers League, "Consumers Face Online Holiday Shopping Season with Credit Card Worries, Misconceptions, NCL Survey Shows" 3 October, http://www.nclnet.org/shoppr1001.htm.

Wolverton, Troy (2001), "Study: More Anti-Fraud Measures Needed", *ZDnet News*, 20 January, http://www.zdnet.com/zdnn/stories/news/0,4586,2676754,00.html.

NOTES

1. The final report of The Hague conference is available on the OECD consumer policy Web site at: http://www.oecd.org/sti/consumer-policy.

2. The final report of the Berlin workshop is available on the OECD consumer policy Web site at: http://www.oecd.org/sti/sti/consumer-policy.

3. For more B2C statistics, see also "Business-to-Consumer E-Commerce Statistics", an addendum to John Dryden's (Head of Information, Computer and Communications Policy Division, OECD Secretariat) presentation at the Berlin workshop, 13-14 March 2001, http://www.oecd.org/pdf/M00001000/M00001293.pdf.

4. See http://www.ftc.gov/bcp/workshops/security/comments/visa.pdf.

5. In a report to the OECD for the March 2001 Berlin workshop, the IMSN said that data from its 14-15 February 2001 sweep of 3 271 sites worldwide showed that 55.89% of them provided a policy on returns, exchanges and refunds. The IMSN called this an area "which may be targeted globally for improvement." (The report did note that on sites where a returns, exchanges and refunds policy was displayed, 97.15% allowed returns, exchanges and refunds.) The IMSN report is included in the final report of the Berlin workshop, which is available on the OECD consumer policy Web site at: http://www.oecd.org/sti/consumer-policy.

6. For more information about "Verified by Visa", see http://www.visa.com/verified.

7. To date, effective and performant AVS are not available in all countries and rarely in cross-border situations.

8. Figures provided by Visa USA indicate that, of the approximately 28 million Visa Internet transactions processed worldwide in April 2000, less than one-half of 1% were charged back as unauthorised. See Russell Schrader's testimony at the Federal Trade Commission – Department of Commerce workshop, Alternative Dispute Resolution for Online Consumer Transactions in the Borderless Online Marketplace, 6 June 2000, p.147, http://www.ftc.gov/bcp/altdisresolution/00606adr.pdf.

9. See American Express' public comment, as posted at the FTC Workshop: US Perspectives on Consumer Protection in the Global Electronic Marketplace Web site; 30 June 1999 http://www.ftc.gov/bcp/icpw/comments/americanexpress.htm.

10. See http://www.usa.visa.com/personal/secure_with_visa/zero_liability.html.

11. See http://www.mastercard.com/general/zero_liability.html .

12. See American Express' public comment, as posted at the FTC Workshop: US Perspectives on Consumer Protection in the Global Electronic Marketplace Web site, 30 June 1999, http://www.ftc.gov/bcp/icpw/comments/americanexpress.htm.

13. Next Card offered such protection as of 1999. See http://www.nextcard.com.

14. Providian National Bank makes such an offer. See https://www.mysmartvisa.com/.

15. Offer of CapitalOne, *Washington Post*, 24 October 2000, p.E6, copy available upon request.

16. See http://http://www.commbank.com.au.

17 See http://www.westpac.com.au.

18. Examples include *Directive 97/7 of 20 May 1997 on the protection of consumers in respect of distance contracts, Official Journal L 144*, 4 June 1991, p. 0019-0027; *Council Directive 87/102/EEC of 22 December 1986 for the approximation of the laws, regulations and administrative provisions of the Member States concerning consumer credit, Official Journal L 042*, 12 February 1987, p. 004–0053 (with corrigendum in *Official Journal* L 278, 11 October 1988, p. 0033; *Commission Recommendation*

97/489/EC of 30 July 1997 concerning transactions by electronic payment instruments and in particular the relationship between issuer and holder, *Official Journal L 208*, 2 August 1997, p. 0052–0058. With regard to payment by card (the predominant way of making payments in a business-to-consumer electronic commerce environment) Directive 97/7 provides that a consumer should be allowed to request cancellation of a payment where fraudulent use has been made of his payment card in connection with distance contracts covered by the Directive; and to be re-credited with the sums paid or have them returned, in the event of fraudulent use. If the price of goods or services is fully or partly covered by credit granted by the supplier, or if that price is fully or partly covered by credit granted to the consumer by a third party on the basis of an agreement between the third party and the supplier, the credit agreement will be cancelled, without penalty, if the consumer exercises his right to withdraw from the contract.

19. Information on the Fraud Prevention Action Plan is available online at: http://europa.eu.int/comm/internal_market/en/finances/payment/fraud/cardfraud.htm. Information on the Communication on E-Commerce and Financial Services is available online at: http://europa.eu.int/comm/internal_market/en/finances/general/ecom.htm.

ANNEX

USING PAYMENT CARDS ONLINE:
FREQUENTLY ASKED QUESTIONS (FAQS)

These frequently asked questions (FAQs) were developed by the OECD's Committee on Consumer Policy, in consultation with experts from consumer groups and the business community. They are intended to educate consumers about the online use of credit and debit cards issued in any of the OECD's 30 Member countries. However, there are important differences in the laws and business practices within these countries, so consumers should read their cardholder agreements carefully and consult the additional informational resources provided under Question 12.

General concerns about the safety of using payment cards online

Question 1. ***Is it safe to use a credit card (pay later) online?***

A. In general, it is just as safe to use a credit card online as off line. In fact, under the laws of some OECD countries, you have no liability if your card is used online without your permission. Card issuers may also offer protections for your online transactions. If you notice a charge for a purchase that you did not make or authorise, you should contact your card issuer immediately (by phone and by letter), question the charge, and ask the issuer to have the charge removed from your account.

Even with the protections offered by some governments and card issuers, it is important to be cautious when you use your credit card online. For example, use a secure browser (see Question 8) and look for a Web site's policy about the privacy and security of your payment card information. Read it. If it does not meet your personal privacy or security standards, consider doing business with another Web site.

Question 2. ***Is it safe to use a debit card (pay now) online?***

A. In general, it is wise to use the same care online to protect your account information, including your PIN code, as you would offline. When you use a debit card, the payment amount is taken out of your account almost immediately. If a problem occurs, your account can be emptied very fast. That means that mistakes or unauthorised uses may occur initially at your expense, rather than the card issuer's expense. Many OECD countries limit your liability for the unauthorised use of your debit card if you report the problem promptly, and a few countries provide additional protections as well. Many debit card issuers also offer protections against the unauthorised use of your debit card.

As always, even with the protections offered by some governments and card issuers, just as with offline transactions, it is important to be cautious when you use your debit card online. For example, use a secure browser (see Question 8) and look for a Web site's policy about the privacy and security of your payment card information. Read it. If it doesn't meet your personal privacy or security standards, consider doing business with another Web site.

Question 3. ***How safe is it to send payment card information in an e-mail?***

A. Messages sent by e-mail have no special security protections. Be wary of including your payment card information in an e-mail.

Special protections offered to payment cardholders

Question 4. ***If someone else uses my payment card to buy something on the Internet and I did not authorise the purchase, do I have to pay? If yes, for how much am I liable?***

A. As a payment cardholder, you have many protections against the unauthorised use of your payment card. Many OECD countries have laws that limit your liability for unauthorised transactions, and some card issuers provide additional protections voluntarily. These protections are implemented in a variety of ways. In some cases, you may be liable for a portion of the unauthorised charge; in others your liability may depend on when and how you notify your card issuer. Contact consumer protection authorities in your country or your card issuer to find out what protections you have and how to use them.

Question 5. ***If I buy something on a Web site using a payment card, but I don't receive the product, do I have to pay? What can I do if the product I ordered is not what I get? What do I do if I am billed for the wrong item on my payment card account statement?***

A. Some OECD countries have laws protecting payment cardholders in the event of non-delivery or delivery of the wrong item. In some cases, card issuers provide protections. These protections may differ depending on the type of payment card used. In either case, you may want to contact the merchant to try to resolve your problem directly. You can also contact the card issuer.

Question 6. ***If I use a payment card to buy something on a Web site and I am unhappy with the quality, what can I do?***

A. Cardholder protections against problems related to the quality of goods purchased online are less common. Your best bet is to do what you would do offline: try to resolve the issue directly with the merchant. If you are not successful, contact your card issuer. Legal protections may apply in some countries. In some countries, such protections differ depending on the type of payment card used. You might also consider alternative dispute resolution. If you are not successful in resolving your grievance, you can complain to a law enforcement agency.

Question 7. ***What can I do if the amount on my payment card statement is different from the amount specified by the Web site when I made my purchase?***

A. Read your monthly statements promptly. Contact the online merchant and ask that the discrepancy be explained or fixed. You can also contact the payment card issuer by letter to ask that the discrepancy be fixed. Keeping good records about your transactions, including print-outs of your purchase confirmation pages, should help you resolve any errors.

Understanding the online payment process

Question 8. ***When I use a payment card to buy online, how do I know how safe my payment card information is?***

A. Generally, if you use a secure browser, transmission of your payment card information will more likely be safe. A secure browser is one that supports a security measure called SSL (Secure Sockets Layer), which encodes and protects your data before it leaves your computer. Most major browsers (for example, Internet Explorer and Netscape Communicator) support SSL. Also:

- Think about limiting your transactions to Web merchants that use security measures like SSL. To verify this feature, make sure the Web address (URL) for the order form begins with "https:" instead of "http:"

- Prior to submitting payment information, look for an icon (for example, a closed padlock or a key) on the bottom of your computer screen to signal that your transmission will be secure.

- Remember that messages sent by e-mail do not benefit from special security protections, so be wary of including payment card information in an e-mail.

- As always, before you provide your payment card information online, check the Web site's privacy and security policies. Look for an explanation about what personal information the site collects, how that information is used, and whether the information is shared with other companies working with the Web site, marketers, or others. If you cannot find a privacy policy, consider whether you want to do business with that company.

Question 9. ***Sometimes, just as I am about to provide information to a Web site, a window pops up that says I am about to enter a secure Web site. Other times, there is a message that says I am about to enter a non-secure Web site. What do these messages mean?***

A. Your browser generates these messages to tell you about the security of transmission of your information. The first type of message signals that you are about to make a secure connection to the Web site. Once the connection is secured, the information that you provide to the Web site (for example, your payment card information) will be encoded so that it can't be read while in transit. The second type of message indicates that you are leaving the secure connection. Be wary about divulging any payment card information unless you have a secure connection.

Question 10. ***When I am in the middle of a transaction and I input payment card details into the spaces provided by the Web site, can my information be accessed by others if I hit the "back" button? If my computer crashes when I'm in the middle of a transaction, is my information still secure?***

A. The information that you type usually doesn't leave your computer until you click the appropriate button to send your payment details. Whether you use your "back" button or your computer crashes, your payment card details generally are in your control until you decide to send them to the online merchant.

However, at a public computer or at a computer you share with someone else, such as at a library or Internet café, the information you type may be more accessible. Be more cautious about releasing your financial information in this situation and review your monthly statements carefully for possible unauthorised charges.

Question 11. ***Where does my information go once the transaction has been completed and how do I know that it has been stored securely?***

A. Once your transaction is completed, your financial details are sent to the online merchant. Security measures like SSL help ensure the safe delivery of your information to the merchant. But remember that they do not ensure its security afterwards. The security of your online information depends on the merchant. Many online merchants explain their security procedures and policies on their Web sites. Review the information before you place an order. Also consider the privacy policy of the online merchant regarding whether they share your information with other companies working with the Web site, marketers, or others.

For more information

Question 12. ***Where can I get more information?***

A. The Web puts many resources at your fingertips:

- For educational initiatives related to electronic commerce in OECD countries:

  http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-countrylist-44-1-no-no-106-0,FF.html

- To locate consumer protection authorities in OECD countries:

  http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-countrylist-44-1-no-no-100-0,FF.html

- To file a complaint about cross-border e-commerce with those authorities, or get tips about safe online shopping:

  http://www.econsumer.gov

- For information about online alternative dispute resolution:

  http://www.oecd.org/oecd/pages/home/displaygeneral/0,3380,EN-document-44-1-no-20-1300-0,FF.html

- For additional information about consumer policy at the OECD, visit:

  http://www.oecd.org/sti/consumer-policy